Clarifier les actions de règle de politique de contrôle d’accès de Firepower Threat Defense

Contenu

Introduction

Ce document décrit les différentes actions disponibles sur la politique de contrôle d'accès et la politique de préfiltre de Firepower Threat Defense (FTD).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Décharge de flux
- Captures de paquets sur les appliances Firepower Threat Defense
- Traceur de paquet et capture avec option de trace sur les appareils Firepower Threat Defense (FTD)

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Firepower 4110 Threat Defense version 6.4.0 (build 113) et 6.6.0 (build 90)
- Centre de gestion Firepower Management Center (FMC) version 6.4.0 (build 113) et 6.6.0 (build 90)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Produits connexes

Ce document peut également être utilisé avec les versions matérielles et logicielles suivantes :

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR1000, FPR2100, FPR4100, FPR9300
- VMware (ESXi), Amazon Web Services (AWS), machine virtuelle à base de noyau (KVM)
- Module de routeur à services intégrés (ISR)
- Logiciel Firepower Threat Defense (FTD) versions 6.1.x et ultérieures

> **Note**: Le flux de déchargement est pris en charge uniquement sur les instances natives des applications Cisco Adaptative Security Appliance (ASA) et Cisco Firepower Threat Defense (FTD) et sur les plateformes FPR4100 et FPR9300. Les instances de conteneur FTD ne prennent pas en charge le déchargement de flux.

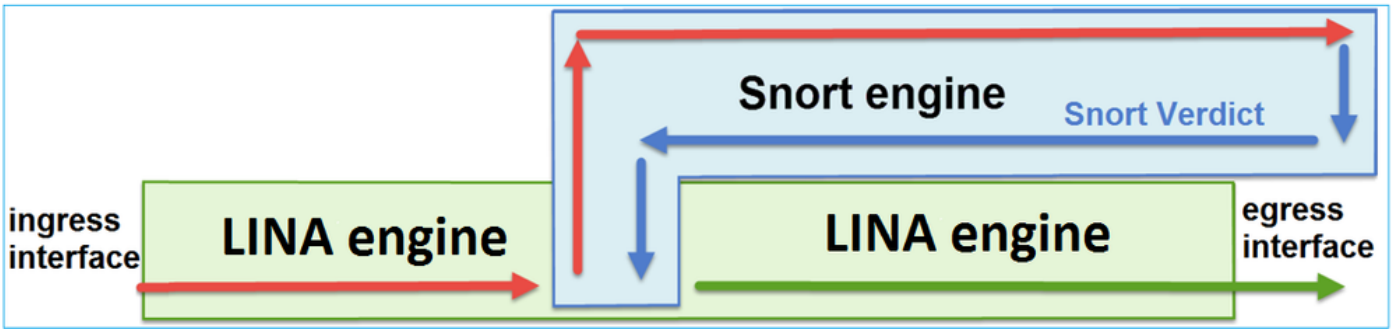
Informations générales

Le fonctionnement en arrière-plan de chaque action est examiné, ainsi que son interaction avec d'autres fonctionnalités telles que le déchargement de flux et les protocoles qui ouvrent des connexions secondaires.

Cisco Firepower Threat Defense (FTD) est une image logicielle unifiée qui comprend deux moteurs principaux :

- Moteur LINA
- Moteur du renifleur

Cette figure montre comment les deux moteurs interagissent :



- Un paquet entre dans l'interface d'entrée et est géré par le moteur LINA
- Si cela est requis par la politique FTD, le paquet est inspecté par le moteur du renifleur
- Le moteur Snort renvoie un verdict (liste d'autorisation ou liste de blocage) pour le paquet
- Le moteur LINA abandonne ou transfère le paquet en fonction du verdict du renifleur

Mode de déploiement de la politique de contrôle d'accès

La politique FTD est configurée sur Cisco Firepower Management Center (FMC) lorsque la gestion par défaut (à distance) est utilisée ou sur Firepower Device Manager (FDM) lorsque la gestion locale est utilisée. Dans les deux cas, la politique de contrôle d'accès est déployée comme :

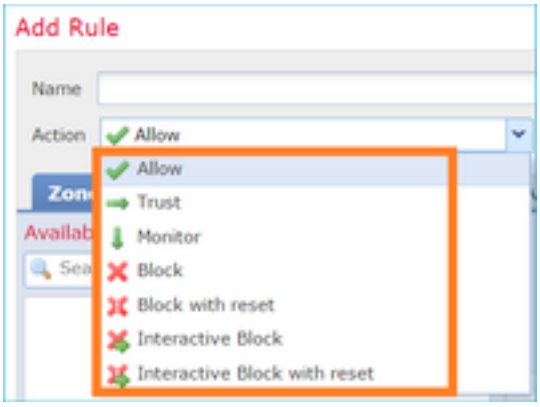
- Une liste de contrôle d'accès (ACL) globale nommée CSM_FW_ACL_ au moteur FTD LINA
- Des règles de contrôle d'accès dans le fichier /ngfw/var/sf/detection_engines/<UUID>/ngfw.rules du moteur FTD du renifleur

Configuration

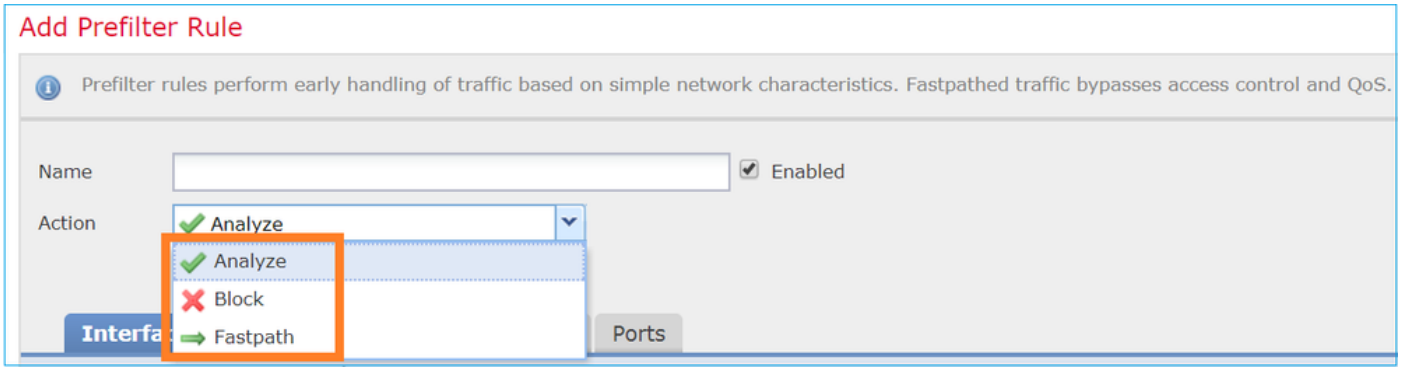
Actions disponibles pour la politique de contrôle d'accès

La politique de contrôle d'accès FTD contient une ou plusieurs règles, et chaque règle peut avoir une de ces actions et comme le montre l'image :

- **Allow**
- **Trust**
- **Monitor**
- **Block**
- **Block with reset**
- **Interactive Block**
- **Interactive Block with reset**



De même, une politique de préfiltre peut contenir une ou plusieurs règles, et les actions possibles sont montrées dans l'image :



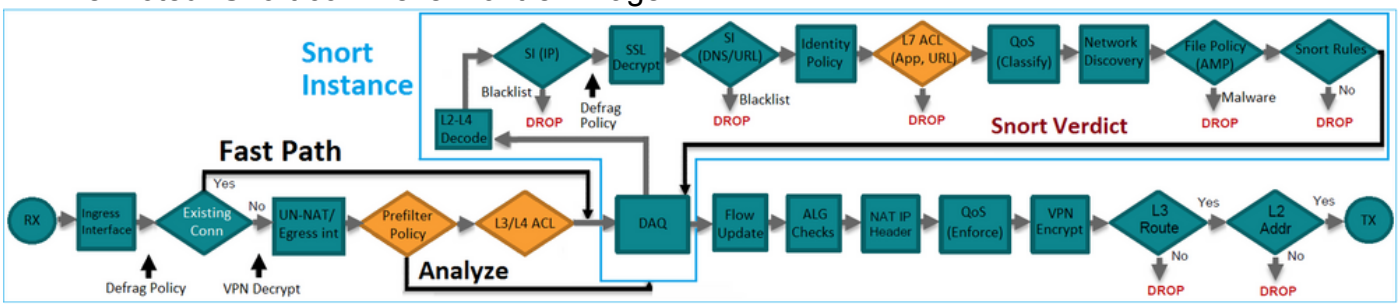
Interactions entre les politiques de contrôle d'accès et de préfiltre

La politique de préfiltrage a été introduite dans la version 6.1 et sert 2 objectifs principaux :

1. Elle permet l'inspection du trafic en tunnel où le moteur FTD LINA vérifie l'en-tête IP externe tandis que le moteur du renifleur vérifie l'en-tête IP interne. Plus précisément, dans le cas du trafic tunnelisé (par exemple GRE), les règles de la stratégie de préfiltrage agissent toujours sur le **outer headers**, tandis que les règles de l'ACP sont toujours applicables aux sessions internes **(inner headers)**. Le trafic en tunnel se reporte à ces protocoles :

- GRE
- IP-en-IP
- IPv6-en-IP
- Port Teredo 3544

2. Il fournit un contrôle d'accès anticipé (EAC) qui permet au flux de contourner complètement le moteur Snort comme le montre l'image.



Les règles de préfiltrage sont déployées sur FTD en tant qu'éléments de contrôle d'accès (ACE)

de couche 3/4 et précèdent les ACE configurés de couche 3/4, comme illustré dans l'image :

```
firepower# show access-list
access-list CSM_FW_ACL_ line 1 remark rule-id 268434457: PREFILTER POLICY: FTD_Prefilter_Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 268434457: RULE: Fastpath_Rule1
access-list CSM_FW_ACL_ line 3 advanced trust ip host 192.168.75.16 any rule-id 268434457 event-log both (hitcnt=0)
access-list CSM_FW_ACL_ line 4 remark rule-id 268434456: PREFILTER POLICY: FTD_Prefilter_Policy
access-list CSM_FW_ACL_ line 5 remark rule-id 268434456: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 6 advanced permit ipinip any any rule-id 268434456 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 7 advanced permit 41 any any rule-id 268434456 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 8 advanced permit gre any any rule-id 268434456 (hitcnt=2) 0x52c7a066
access-list CSM_FW_ACL_ line 9 advanced permit udp any any eq 3544 rule-id 268434456 (hitcnt=0) 0xcf6309bc
access-list CSM_FW_ACL_ line 10 remark rule-id 268434445: ACCESS POLICY: FTD5506-1 - Mandatory/1
access-list CSM_FW_ACL_ line 12 advanced deny ip host 10.1.1.1 any rule-id 268434445 event-log flow-start (hitcnt=0) 0x8bf72c63
access-list CSM_FW_ACL_ line 14 remark rule-id 268434434: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ line 15 advanced permit ip any any rule-id 268434434 (hitcnt=410) 0xa1d3780e
```

Prefilter Rules

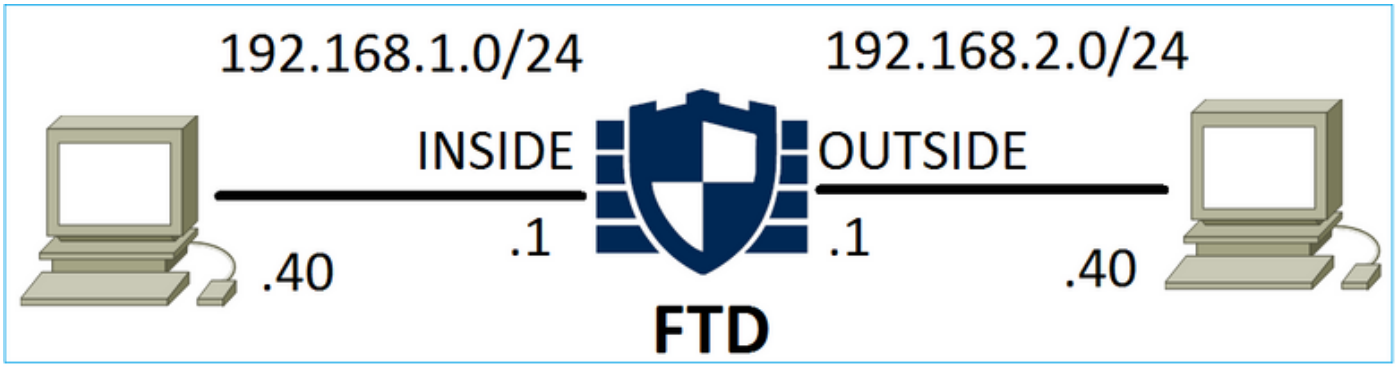
Tunnel Prefilter Rules

L3/L4 ACEs

Note: Préfiltre contre règles de la politique de contrôle d'accès = la première correspondance est appliquée.

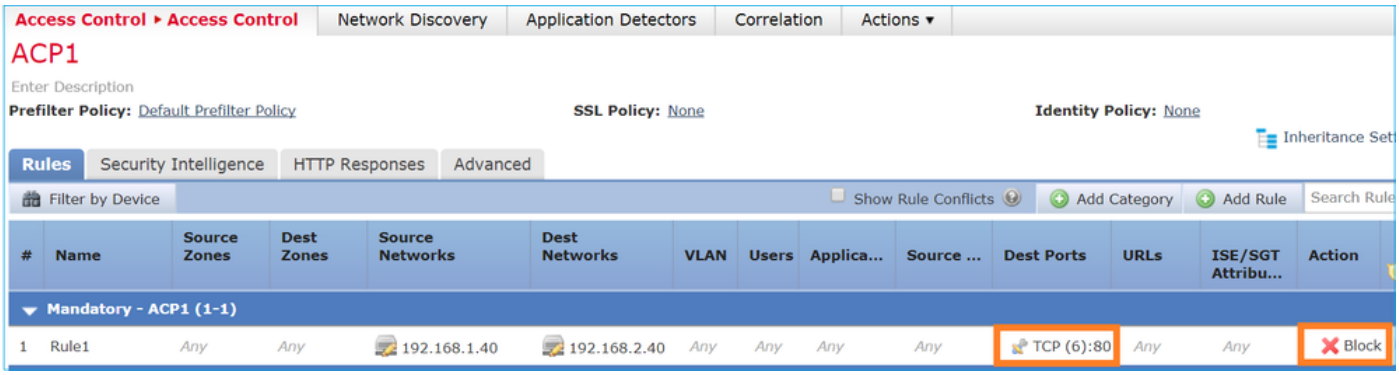
Action Block (blocage) de la politique de contrôle d'accès

Examinez la topologie présentée dans cette image :



Scénario 1. Abandon LINA précoce

La politique de contrôle d'accès contient une règle de blocage qui utilise une condition L4 (port de destination TCP 80), comme le montre l'image :



La politique déployée dans le renifleur :

```
268435461 deny any 192.168.1.40 32 any any 192.168.2.40 32 80 any 6
```

La politique déployée dans LINA. Notez que la règle est poussée comme **deny** action :

```
firepower# show access-list
```

```
…
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L4 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced deny tcp host 192.168.1.40 host 192.168.2.40 eq www
rule-id 268435461 event-log flow-start (hitcnt=0) 0x6149c43c
```

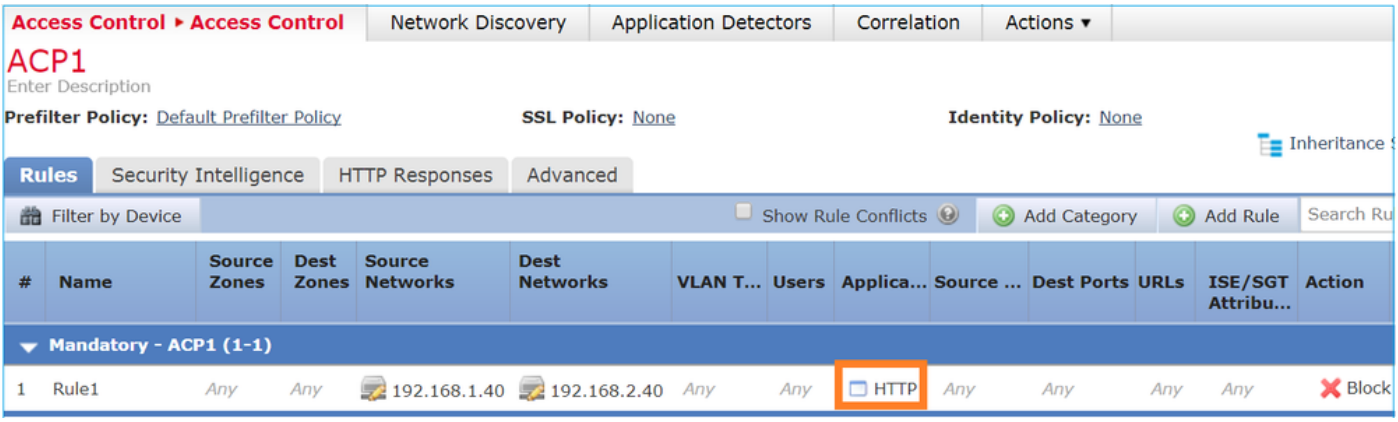
Vérifiez le comportement :

Lorsque l'hôte A (192.168.1.40) tente d'ouvrir une session HTTP vers l'hôte B (192.168.2.40), les paquets de synchronisation TCP (SYN) sont abandonnés par le moteur FTD LINA et n'atteignent pas le moteur Snort ou la destination :

```
firepower# show capture
capture CAPI type raw-data buffer 33554432 trace trace-count 100 interface INSIDE [Capturing -
430 bytes]
  match ip host 192.168.1.40 any
capture CAPO type raw-data buffer 33554432 trace trace-count 100 interface OUTSIDE [Capturing -
0 bytes]
  match ip host 192.168.1.40 any


firepower# show capture CAPI
   1: 11:08:09.672801  192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
<mss 1460,sackOK,timestamp 4060517 0>
   2: 11:08:12.672435  192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
<mss 1460,sackOK,timestamp 4063517 0>
   3: 11:08:18.672847  192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
<mss 1460,sackOK,timestamp 4069517 0>
   4: 11:08:30.673610  192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
<mss 1460,sackOK,timestamp 4081517 0>


firepower# show capture CAPI packet-number 1 trace
   1: 11:08:09.672801  192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
<mss 1460,sackOK,timestamp 4060517 0>
...

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny tcp host 192.168.1.40 host 192.168.2.40 eq www rule-id
268435461 event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268435461: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268435461: L4 RULE: Rule1
Additional Information:
                              <- No Additional Information = No Snort Inspection

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

Scénario 2. Abandon en raison d'un verdict Snort

La politique de contrôle d'accès contient une règle de blocage qui utilise une condition L7 (Application HTTP), comme le montre l'image :



La politique déployée dans le renifleur :

```
268435461 deny any 192.168.1.40 32 any any 192.168.2.40 32 any any any  (appid 676:1)
```

Appid 676:1 = HTTP

La politique déployée dans LINA.

> **Note**: La règle est poussée comme un **permit** car LINA ne peut pas déterminer que la session utilise HTTP. Sur FTD, le mécanisme de détection des applications est dans le moteur Snort.

```
firepower# show access-list
…
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L7 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435461 (hitcnt=0) 0xb788b786
```

Pour une règle de blocage qui utilise **Application** comme condition, la trace d'un paquet réel montre que la session est abandonnée par le LINA en raison du verdict du moteur Snort.

> **Note**: Pour que le moteur de renifleur puisse déterminer l'application, il doit inspecter quelques paquets (généralement de 3 à 10, selon le décodeur de l'application). Ainsi, quelques paquets sont autorisés à traverser Cisco FTD et arrivent à destination. Les paquets autorisés sont toujours soumis à la vérification de la stratégie d'intrusion basée sur **Access Policy > Advanced > 'Intrusion Policy used before Access Control rule is determined'** option.

Vérifiez le comportement :

Lorsque l'hôte A (192.168.1.40) tente d'établir une session HTTP avec l'hôte B (192.168.2.40), la saisie d'entrée LINA indique :

```
firepower# show capture CAPI
```

```
8 packets captured

   1: 11:31:19.825564  192.168.1.40.32790 > 192.168.2.40.80: S 357753151:357753151(0) win 2920
<mss 1460,sackOK,timestamp 5450579 0>
   2: 11:31:19.826403  192.168.2.40.80 > 192.168.1.40.32790: S 1283931030:1283931030(0) ack
357753152 win 2896 <mss 1380,sackOK,timestamp 5449236 5450579>
   3: 11:31:19.826556  192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5450580 5449236>
   4: 11:31:20.026899  192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5450781 5449236>
   5: 11:31:20.428887  192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5451183 5449236>
 ...
```

La saisie de sortie :

```
firepower# show capture CAPO

5 packets captured

   1: 11:31:19.825869  192.168.1.40.32790 > 192.168.2.40.80: S 1163713179:1163713179(0) win 2920
<mss 1380,sackOK,timestamp 5450579 0>
   2: 11:31:19.826312  192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5449236 5450579>
   3: 11:31:23.426049  192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5452836 5450579>
   4: 11:31:29.426430  192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5458836 5450579>
   5: 11:31:41.427208  192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5470836 5450579>
```

La trace indique que le premier paquet (TCP SYN) est autorisé par le Snort puisque le verdict de détection d'application n'a pas encore été atteint :

```
firepower# show capture CAPI packet-number 1 trace
   1: 11:31:19.825564  192.168.1.40.32790 > 192.168.2.40.80: S 357753151:357753151(0) win 2920
<mss 1460,sackOK,timestamp 5450579 0>
...

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435461
access-list CSM_FW_ACL_ remark rule-id 268435461: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268435461: L7 RULE: Rule1
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will be reached
...
Phase: 10
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 23194, packet dispatched to next module
```

```
…
Phase: 12
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: TCP, SYN, seq 357753151
AppID: service unknown (0), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 0, icmpCode 0
Firewall: pending rule-matching, id 268435461, pending AppID
NAP id 1, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet

Result:
input-interface: OUTSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow
```

De même pour le paquet TCP SYN/ACK :

```
firepower# show capture CAPO packet-number 2 trace
   2: 11:31:19.826312 192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5449236 5450579>
…

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found flow with id 23194, using existing flow
…

Phase: 5
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: TCP, SYN, ACK, seq 1283931030, ack 357753152
AppID: service unknown (0), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 0, icmpCode 0
Firewall: pending rule-matching, id 268435461, pending AppID
NAP id 1, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: INSIDE
output-status: up
```

```
output-line-status: up
Action: allow
```

Snort retourne un verdict DROP une fois qu'une inspection du troisième paquet est terminée :

```
firepower# show capture CAPI packet-number 3 trace
   3: 11:31:19.826556  192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5450580 5449236>

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found flow with id 23194, using existing flow

Phase: 5
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: TCP, ACK, seq 357753152, ack 1283931031
AppID: service HTTP (676), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0(0) -> 0, vlan 0, sgt 65535, user 9999997,
url http://192.168.2.40/128k.html
Firewall: block rule, id 268435461, drop
Snort: processed decoder alerts or actions queue, drop
NAP id 1, IPS id 0, Verdict BLOCKLIST, Blocked by Firewall
Snort Verdict: (block-list) block list this flow

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
Action: drop
Drop-reason: (firewall) Blocked by the firewall preprocessor
```

Vous pouvez également exécuter la commande **system support trace** à partir du mode FTD CLISH. Cet outil offre deux fonctions :

- Affiche le verdict Snort pour chaque paquet lorsqu'il est envoyé à la bibliothèque d'acquisition de données (DAQ) et vu dans LINA. La bibliothèque est un composant situé entre le moteur FTD LINA et le moteur de renifleur
- Permet d'exécuter **system support firewall-engine-debug** en même temps pour voir ce qui se passe dans le moteur Snort lui-même

Voici la sortie :

```
> system support trace

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.1.40
Please specify a client port:
Please specify a server IP address: 192.168.2.40
Please specify a server port:
```

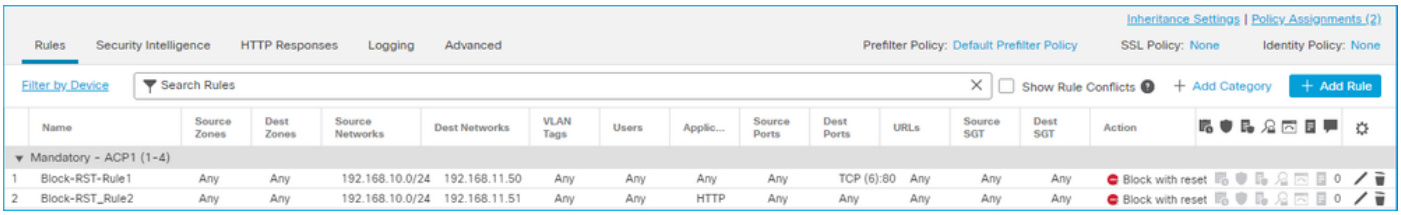
```
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages

Tracing enabled by Lina
192.168.2.40-80 - 192.168.1.40-32791 6 Packet: TCP, SYN, seq 2620409313
192.168.2.40-80 - 192.168.1.40-32791 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 New session
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Rule1', and SrcZone
first with zones -1 -> -1, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0,
payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 ->
0, vlan 0, sgt 65535, user 9999997, icmpType 0, icmpCode 0
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 pending rule order 2, 'Rule1', AppID
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: pending rule-matching, 'Rule1', pending AppID
192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
Trace buffer and verdict reason are sent to DAQ's PDTS

Tracing enabled by Lina
192.168.2.40-80 - 192.168.1.40-32791 6 Packet: TCP, SYN, ACK, seq 3700371680, ack 2620409314
192.168.2.40-80 - 192.168.1.40-32791 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Rule1', and SrcZone
first with zones -1 -> -1, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0,
payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 ->
0, vlan 0, sgt 65535, user 9999997, icmpType 0, icmpCode 0
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 pending rule order 2, 'Rule1', AppID
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: pending rule-matching, 'Rule1', pending AppID
192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
Trace buffer and verdict reason are sent to DAQ's PDTS

Tracing enabled by Lina
192.168.2.40-80 - 192.168.1.40-32791 6 Packet: TCP, ACK, seq 2620409314, ack 3700371681
192.168.2.40-80 - 192.168.1.40-32791 6 AppID: service HTTP (676), application unknown (0)
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Rule1', and SrcZone
first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc
676, payload 0, client 686, misc 0, user 9999997, url http://192.168.2.40/128k.html, xff
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0(0)
-> 0, vlan 0, sgt 65535, user 9999997, url http://192.168.2.40/128k.html
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 match rule order 2, 'Rule1', action Block
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 deny action
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: block rule, 'Rule1', drop
192.168.1.40-32791 > 192.168.2.40-80 6 Snort: processed decoder alerts or actions queue, drop
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Deleting session
192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict BLOCKLIST
192.168.1.40-32791 > 192.168.2.40-80 6 ===> Blocked by Firewall
```

Résumé

- L’action de blocage de la politique de contrôle d’accès est déployée en tant que règle permit (permission) ou de deny (refus) dans LINA qui dépend des conditions de la règle
- Si les conditions sont L3/L4, alors le LINA bloque le paquet. Dans le cas du protocole TCP, le premier paquet (TCP SYN) est bloqué
- Si les conditions sont L7, le paquet est transmis au moteur du renifleur pour une inspection approfondie. Dans le cas d’un protocole TCP, quelques paquets sont autorisés par l’intermédiaire de Cisco FTD jusqu’à ce que le renifleur atteigne un verdict. Les paquets autorisés sont toujours soumis à la vérification de la stratégie d'intrusion basée sur **Access Policy > Advanced > 'Intrusion Policy used before Access Control rule is determined'** option.

Action Block (blocage) de la politique de contrôle d’accès avec réinitialisation

Une règle Block (blocage) avec repos configurée sur l'interface utilisateur de Cisco Firepower Management Center (FMC) :



La règle Block with reset est déployée sur le moteur FTD LINA en tant que **permit** et au moteur Snort en tant que **reset** règle :

```
firepower# show access-list
…
access-list CSM_FW_ACL_ line 10 advanced permit tcp 192.168.10.0 255.255.255.0 host
192.168.11.50 eq www rule-id 268438864 (hitcnt=0) 0xba785fc0
access-list CSM_FW_ACL_ line 11 remark rule-id 268438865: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268438865: L7 RULE: Block-RST_Rule2
access-list CSM_FW_ACL_ line 13 advanced permit ip 192.168.10.0 255.255.255.0 host 192.168.11.51
rule-id 268438865 (hitcnt=0) 0x622350d0
```

Moteur du renifleur :

```
admin@firepower:~$ cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules
…
# Start of AC rule.
268438864 reset any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6
# End rule 268438864
268438865 reset any 192.168.10.0 24 any any 192.168.11.51 32 any any any (appid 676:1)
(ip_protos 6, 17)
# End rule 268438865
```

Lorsqu'un paquet correspond à Block with reset rule, FTD envoie un **TCP Reset** paquet ou un **ICMP Type 3 Code 13** Message de destination inaccessible (filtrée administrativement) :

```
root@kali:~/tests# wget 192.168.11.50/file1.zip
--2020-06-20 22:48:10--  http://192.168.11.50/file1.zip
Connecting to 192.168.11.50:80... failed: Connection refused.
```

Voici une capture réalisée sur l'interface d'entrée de Cisco FTD :

```
firepower# show capture CAPI
2 packets captured
1: 21:01:00.977259 802.1Q vlan#202 P0 192.168.10.50.41986 > 192.168.11.50.80: S
3120295488:3120295488(0) win 29200 <mss 1460,sackOK,timestamp 3740873275 0,nop,wscale 7>
2: 21:01:00.978114 802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.41986: R 0:0(0) ack
3120295489 win 0 2 packets shown
```

System support trace dans ce cas, indique que le paquet est abandonné en raison du verdict Snort :

```
> system support trace

Enable firewall-engine-debug too? [n]: y
```

```
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.50
Please specify a client port:
Please specify a server IP address: 192.168.11.50
Please specify a server port:
Monitoring packet tracer and firewall debug messages


192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 3387496622
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 new firewall session
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 using HW or preset rule order 2, 'Block-RST-
Rule1', action Reset and prefilter rule 0
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 HitCount data sent for rule id: 268438864,
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 reset action
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 deleting firewall session flags = 0x0,
fwFlags = 0x0
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: block w/ reset rule, 'Block-RST-
Rule1', drop
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions
queue, drop
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 9, NAP id 1, IPS id 0, Verdict
BLOCKLIST
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 ===> Blocked by Firewall
Verdict reason is sent to DAQ
```

Scénarios :

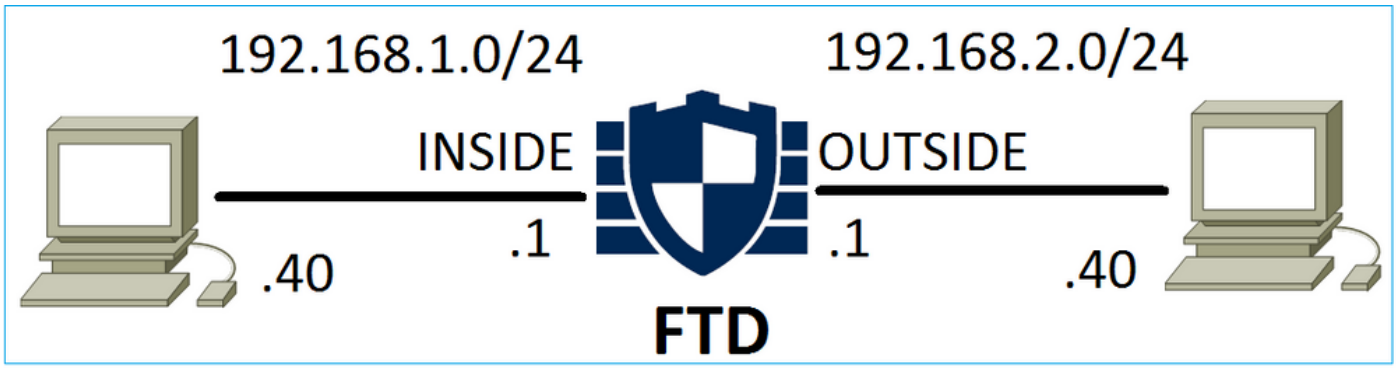
Identique à **Block** , mais met fin immédiatement à la connexion.

Action Allow (autorisation) de la politique de contrôle d'accès

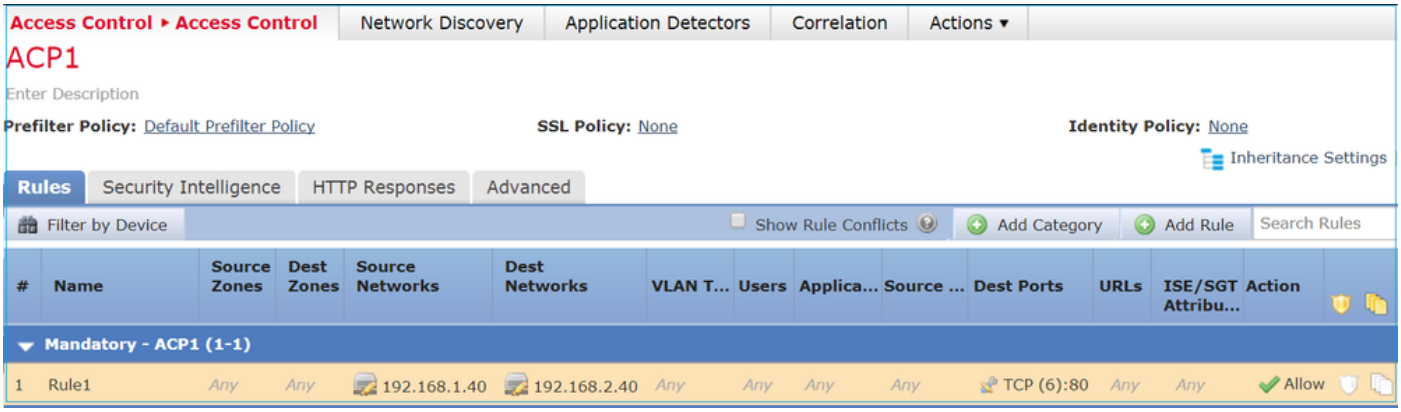
Scénario 1. Action Autoriser ACP (conditions L3/L4)

Normalement, vous devez configurer une règle d'autorisation pour préciser des inspections supplémentaires comme une politique d'intrusion ou une politique de fichiers. Ce premier scénario illustre le fonctionnement d'une règle d'autorisation lorsqu'une condition L3/L4 est appliquée.

Considérez cette topologie comme le montre l'image :



Cette politique est appliquée comme le montre l'image :



La politique déployée dans le renifleur. Notez que la règle est déployée en tant que **allow** action :

```
# Start of AC rule.
268435461 allow any 192.168.1.40 32 any any 192.168.2.40 32 80 any 6
```

La politique de LINA.

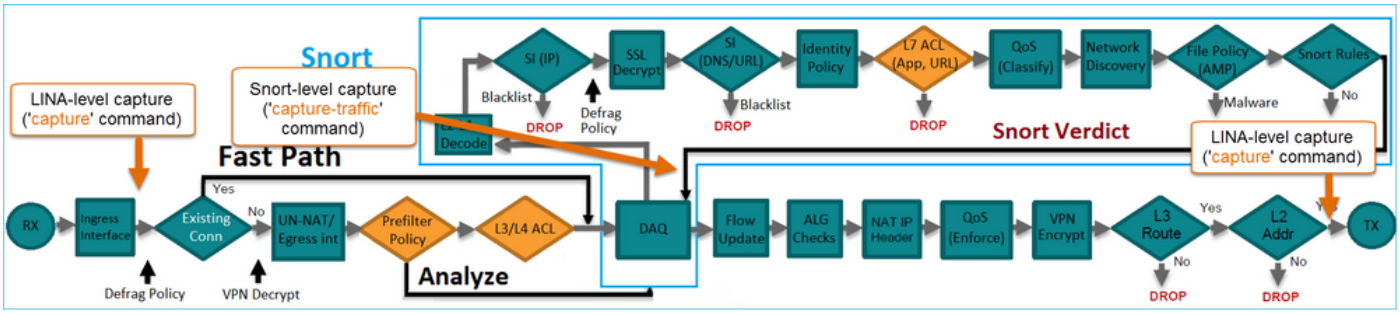
> **Note**: La règle est déployée en tant que **permit** action qui signifie essentiellement la redirection vers Snort pour une inspection plus approfondie.

```
firepower# show access-list
…
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L7 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced permit tcp host 192.168.1.40 host 192.168.2.40 eq www
rule-id 268435461 (hitcnt=1) 0x641a20c3
```

Afin de voir comment FTD gère un flux qui correspond à une règle Allow, il y a quelques façons :

- Vérifier les statistiques du renifleur
- À l'aide de l'outil CLISH de prise en charge du système de trace
- À l'aide de l'utilisation de saisie avec l'option de trace dans LINA et possiblement à l'aide de la capture du trafic dans le moteur du renifleur

Capture LINA c. trafic du renifleur :



Vérifiez le comportement :

Effacer les statistiques Snort, activer **system support trace** from CLISH, and initiate an HTTP flow from host-A (192.168.1.40) to host-B (192.168.2.40). All the packets are forwarded to the Snort engine and get the PASS verdict by the Snort:

```
firepower# clear snort statistics

> system support trace

Please specify an IP protocol:
Please specify a client IP address: 192.168.1.40
Please specify a client port:
Please specify a server IP address: 192.168.2.40
Please specify a server port:
Enable firewall-engine-debug too? [n]:
Monitoring packet tracer debug messages

Tracing enabled by Lina
192.168.2.40-80 - 192.168.1.40-32797 6 Packet: TCP, SYN, seq 361134402
192.168.2.40-80 - 192.168.1.40-32797 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32797 > 192.168.2.40-80 6 Firewall: allow rule, 'Rule1', allow
192.168.1.40-32797 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
Trace buffer and verdict reason are sent to DAQ's PDTS

Tracing enabled by Lina
192.168.2.40-80 - 192.168.1.40-32797 6 Packet: TCP, SYN, ACK, seq 1591434735, ack 361134403
192.168.2.40-80 - 192.168.1.40-32797 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32797 > 192.168.2.40-80 6 Firewall: allow rule, 'Rule1', allow
192.168.1.40-32797 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
Trace buffer and verdict reason are sent to DAQ's PDTS

Tracing enabled by Lina
192.168.2.40-80 - 192.168.1.40-32797 6 Packet: TCP, ACK, seq 361134403, ack 1591434736
192.168.2.40-80 - 192.168.1.40-32797 6 AppID: service HTTP (676), application unknown (0)
192.168.1.40-32797 > 192.168.2.40-80 6 Firewall: allow rule, 'Rule1', allow
192.168.1.40-32797 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
```

Les compteurs de paquets Pass augmentent :

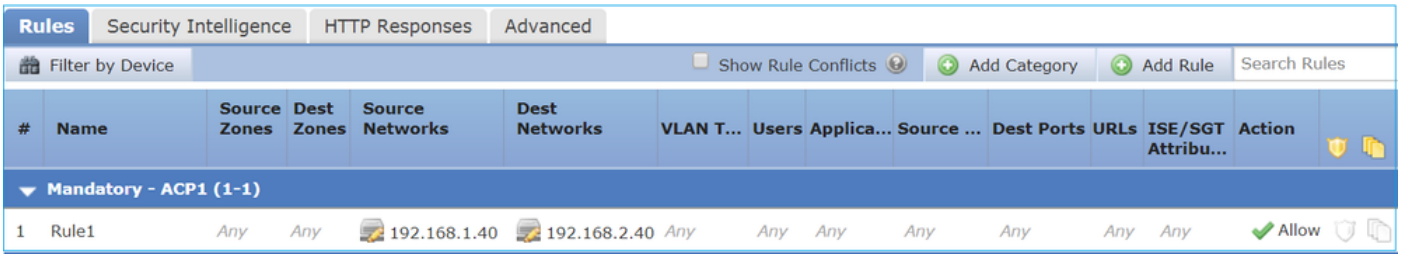
```
> show snort statistics

Packet Counters:
  Passed Packets                                    54
  Blocked Packets                                    0
  Injected Packets                                   0
  Packets bypassed (Snort Down)                      0
  Packets bypassed (Snort Busy)                      0

Flow Counters:
  Fast-Forwarded Flows                               0
  Blocklisted Flows                                  0
...
```

Paquets réussis = inspectés par le moteur de renifleur

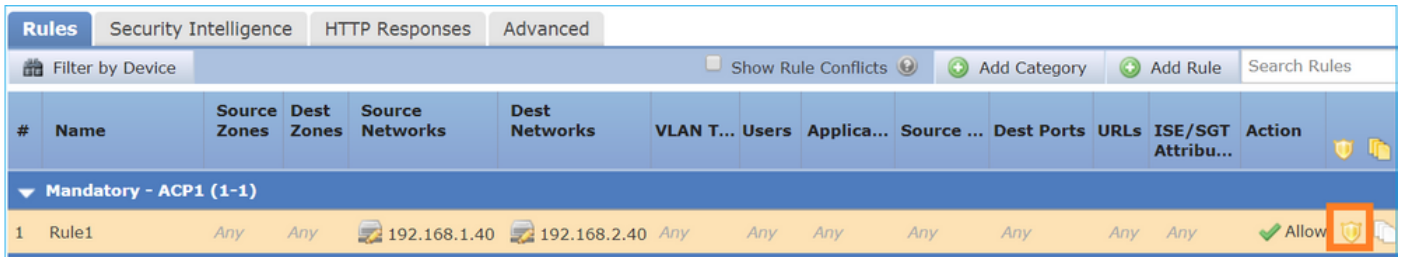
Scénario 2. Action Autoriser ACP (conditions L3-7)

Un comportement similaire se produit lorsque la règle Allow (autorisation) est déployée comme suit.

Seule une condition L3/L4, comme illustré dans l'image :

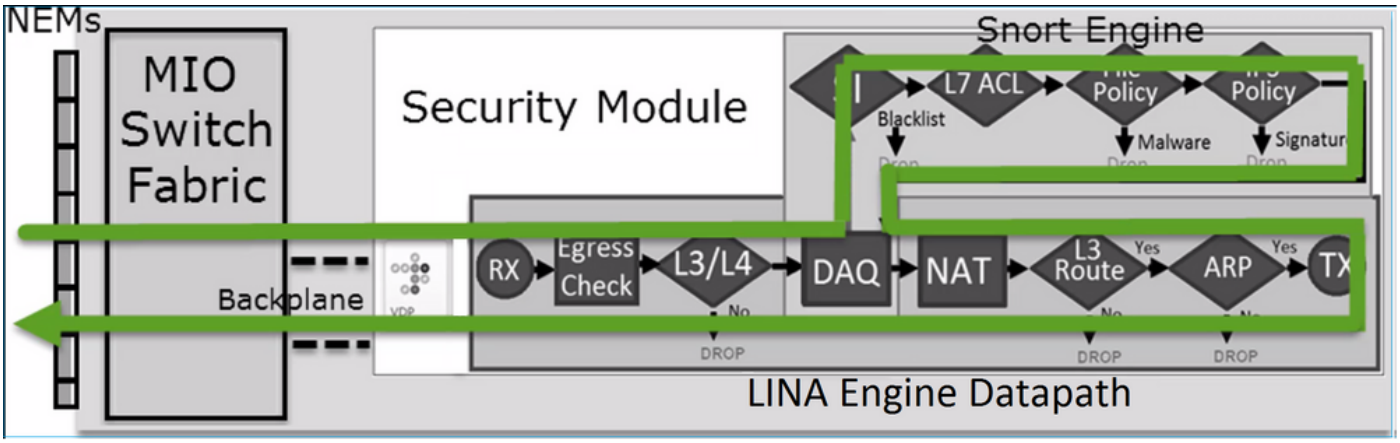


Une condition L7 (par exemple, Intrusion Policy, File Policy, Application, etc.) est affichée dans l'image :



Résumé

En résumé, voici comment un flux est géré par Cisco FTD déployé sur un FP4100/9300 lorsqu'une règle Allow (autorisation) est mise en correspondance, comme le montre l'image :



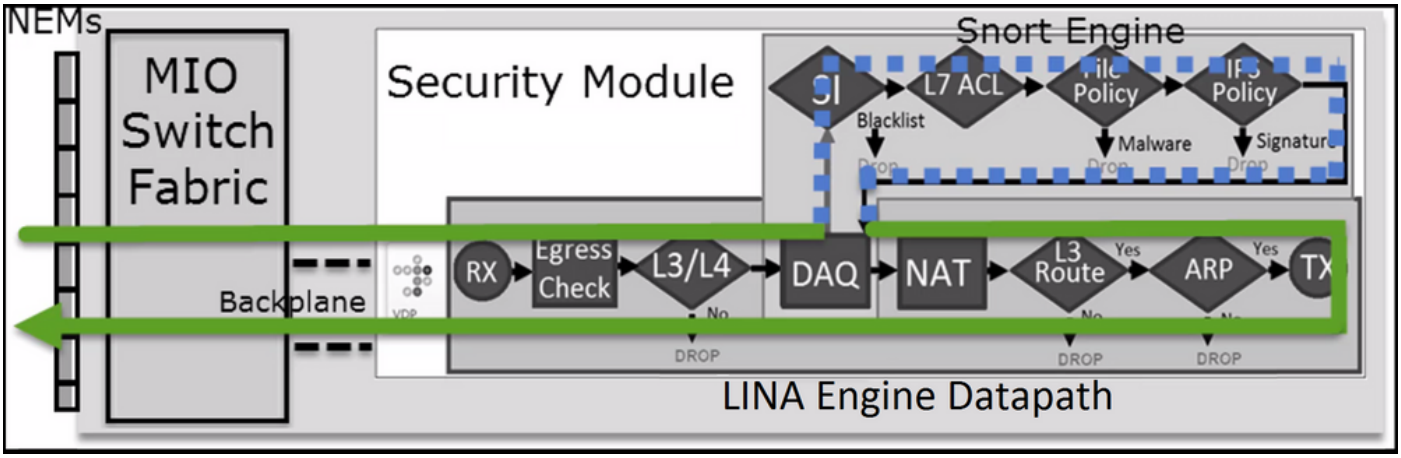
Note: Management Input Output (MIO) est le moteur de supervision du châssis Firepower.

Scénario 3. Arrêt du verdict Fast-Forward avec Allow

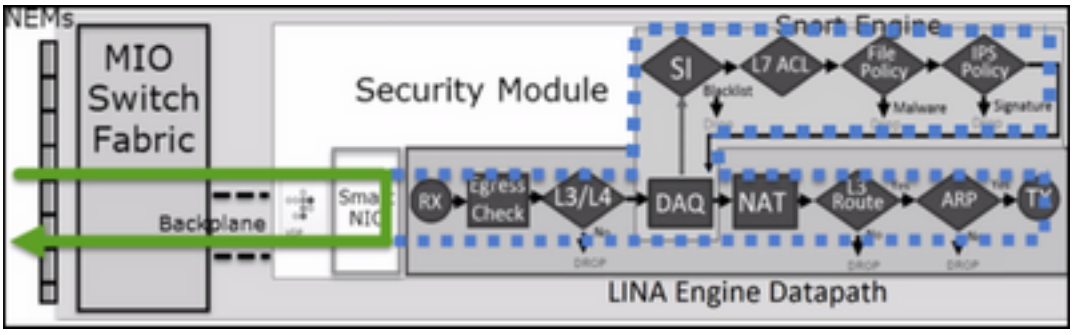
Il existe des scénarios spécifiques où le moteur FTD Snort donne un verdict PERMITLIST (avance rapide) et le reste du flux est déchargé vers le moteur LINA (dans certains cas, il est déchargé vers l'accélérateur matériel - SmartNIC). Ces scénarios sont les suivants :

1. Trafic SSL sans politique SSL configurée
2. Contournement intelligent des applications

Voici la représentation visuelle du chemin du paquet :



Ou dans certains cas :



Points principaux

- La règle d'autorisation est déployée en tant que **allow** dans Snort et **permit** Dans LINA
- Dans la plupart des cas, tous les paquets d'une session sont transférés au moteur Snort pour une inspection supplémentaire

Scénarios :

Vous devez configurer une règle Allow (autorisation) lorsque vous avez besoin d'une inspection L7 par le moteur du renifleur, par exemple :

- Politique d'intrusion
- Politique de fichiers

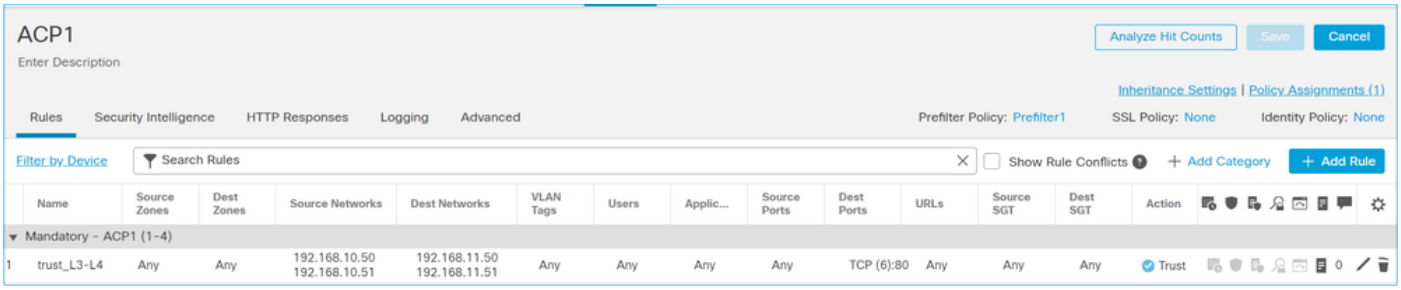
Action Trust (confiance) de la politique de contrôle d'accès

Scénario 1. Action de confiance ACP

Si vous ne souhaitez pas appliquer l'inspection avancée de couche 7 au niveau Snort (par exemple, la stratégie d'intrusion, la stratégie de fichiers, la découverte de réseau), mais que vous souhaitez tout de même utiliser des fonctionnalités telles que Security Intelligence (SI), Identity Policy, QoS, etc., il est recommandé d'utiliser l'action Trust dans votre règle.

Topologie:

La politique configurée :



La règle Trust (confiance) telle qu'elle est déployée dans le moteur FTD de renifleur :

```
# Start of AC rule.
268438858 fastpath any 192.168.10.50 31 any any 192.168.11.50 31 80 any 6 (log dcforward
flowend)
```

Note: Le numéro 6 est le protocole (TCP).

La règle dans FTD LINA :

```
firepower# show access-list | i 268438858
access-list CSM_FW_ACL_ line 17 remark rule-id 268438858: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 18 remark rule-id 268438858: L7 RULE: trust_L3-L4
access-list CSM_FW_ACL_ line 19 advanced permit tcp object-group FMC_INLINE_src_rule_268438858
object-group FMC_INLINE_dst_rule_268438858 eq www rule-id 268438858 (hitcnt=19) 0x29588b4f
  access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.50 host 192.168.11.50 eq
www rule-id 268438858 (hitcnt=19) 0x9d442895
  access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.50 host 192.168.11.51 eq
www rule-id 268438858 (hitcnt=0) 0xd026252b
  access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.51 host 192.168.11.50 eq
www rule-id 268438858 (hitcnt=0) 0x0d785cc4
  access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.51 host 192.168.11.51 eq
www rule-id 268438858 (hitcnt=0) 0x3b3234f1
```

Vérification :

Activer **system support trace** et lancez une session HTTP de l'hôte A (192.168.10.50) vers l'hôte B (192.168.11.50). Trois paquets sont transférés au moteur du renifleur. Snort engine envoie à LINA le verdict PERMITLIST qui décharge essentiellement le reste du flux vers le moteur LINA :

```
> system support trace

Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.50
Please specify a client port:
Please specify a server IP address: 192.168.11.50
Please specify a server port: 80
Monitoring packet tracer and firewall debug messages

192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 453426648
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 new firewall session
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 using HW or preset rule order 5, 'trust_L3-
L4', action Trust and prefilter rule 0
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 HitCount data sent for rule id: 268438858,
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-
L4', allow
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 2, NAP id 2, IPS id 0, Verdict
PASS

192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Packet: TCP, SYN, ACK, seq 2820426532, ack
453426649
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-
L4', allow
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Snort id 2, NAP id 2, IPS id 0, Verdict
PASS

192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 453426649, ack
2820426533
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-
L4', allow
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 2, NAP id 2, IPS id 0, Verdict
PERMITLIST
```

Une fois la connexion terminée, le moteur du renifleur obtient les informations de métadonnées du moteur LINA et supprime la session :

```
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 Got end of flow event from hardware with
flags 00010001. Rule Match Data: rule_id 0, rule_action 0 rev_id 0, rule_flags 3
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 Logging EOF for event from hardware with
rule_id = 268438858 ruleAction = 3 ruleReason = 0
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 : Received EOF, deleting the snort session.

192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: deleting snort session, reason:
timeout
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 deleting firewall session flags = 0x10003,
fwFlags = 0x1115
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: deleted snort session using 0
bytes; protocol id:(-1) : LWstate 0xf LWFlags 0x6007
```

La capture Snort montre les 3 paquets qui vont au moteur Snort :

```
> capture-traffic

Please choose domain to capture traffic from:
  0 - management0
  1 - management1
  2 - Global

Selection? 2

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: -n vlan and (host 192.168.10.50 and host 192.168.11.50)
10:26:16.525928 IP 192.168.10.50.42144 > 192.168.11.50.80: Flags [S], seq 3065553465, win 29200,
options [mss 1380,sackOK,TS val 3789188468 ecr 0,nop,wscale 7], length 0
10:26:16.525928 IP 192.168.11.50.80 > 192.168.10.50.42144: Flags [S.], seq 3581351172, ack
3065553466, win 8192, options [mss 1380,nop,wscale 8,sackOK,TS val 57650410 ecr 3789188468],
length 0
10:26:16.525928 IP 192.168.10.50.42144 > 192.168.11.50.80: Flags [.], ack 1, win 229, options
[nop,nop,TS val 3789188470 ecr 57650410], length 0
```

La capture LINA montre le flux qui la traverse :

```
firepower# show capture CAPI

437 packets captured

   1: 09:51:19.431007  802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: S
2459891187:2459891187(0) win 29200 <mss 1460,sackOK,timestamp 3787091387 0,nop,wscale 7>
   2: 09:51:19.431648  802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: S
2860907367:2860907367(0) ack 2459891188 win 8192 <mss 1380,nop,wscale 8,sackOK,timestamp
57440579 3787091387>
   3: 09:51:19.431847  802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: . ack
2860907368 win 229 <nop,nop,timestamp 3787091388 57440579>
   4: 09:51:19.431953  802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: P
2459891188:2459891337(149) ack 2860907368 win 229 <nop,nop,timestamp 3787091388 57440579>
   5: 09:51:19.444816  802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: .
2860907368:2860908736(1368) ack 2459891337 win 256 <nop,nop,timestamp 57440580 3787091388>
   6: 09:51:19.444831  802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: .
2860908736:2860910104(1368) ack 2459891337 win 256 <nop,nop,timestamp 57440580 3787091388>

…
```

La trace des paquets de LINA est une autre façon de voir les verdicts du renifleur. Le premier paquet a obtenu le verdict PASS (réussite) :

```
firepower# show capture CAPI packet-number 1 trace | i Type|Verdict
Type: CAPTURE
Type: ACCESS-LIST
Type: ROUTE-LOOKUP
Type: ACCESS-LIST
Type: CONN-SETTINGS
Type: NAT
Type: NAT
Type: IP-OPTIONS
Type: CAPTURE
Type: CAPTURE
Type: NAT
Type: CAPTURE
Type: NAT
```

```
Type: IP-OPTIONS
Type: CAPTURE
Type: FLOW-CREATION
Type: EXTERNAL-INSPECT
Type: SNORT
Snort id 22, NAP id 2, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Type: ADJACENCY-LOOKUP
Type: CAPTURE
```

Trace du paquet TCP SYN/ACK sur l'interface OUTSIDE :

```
firepower# show capture CAPO packet-number 2 trace | i Type|Verdict
Type: CAPTURE
Type: ACCESS-LIST
Type: FLOW-LOOKUP
Type: EXTERNAL-INSPECT
Type: SNORT
Snort id 22, NAP id 2, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Type: ADJACENCY-LOOKUP
Type: CAPTURE
```

L'ACK TCP obtient le verdict PERMITLIST :

```
firepower# show capture CAPI packet-number 3 trace | i Type|Verdict
Type: CAPTURE
Type: ACCESS-LIST
Type: FLOW-LOOKUP
Type: EXTERNAL-INSPECT
Type: SNORT
Snort id 22, NAP id 2, IPS id 0, Verdict PERMITLIST
Snort Verdict: (fast-forward) fast forward this flow
Type: CAPTURE
```

Ceci est la sortie complète du verdict du renifleur (paquet n° 3)

```
firepower# show capture CAPI packet-number 3 trace | b Type: SNORT
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: TCP, ACK, seq 687485179, ack 1029625865
AppID: service unknown (0), application unknown (0)
Firewall: trust/fastpath rule, id 268438858, allow
Snort id 31, NAP id 2, IPS id 0, Verdict PERMITLIST
Snort Verdict: (fast-forward) fast forward this flow
```

Le 4e paquet n'est pas transféré au moteur Snort car le verdict est mis en cache par le moteur LINA :

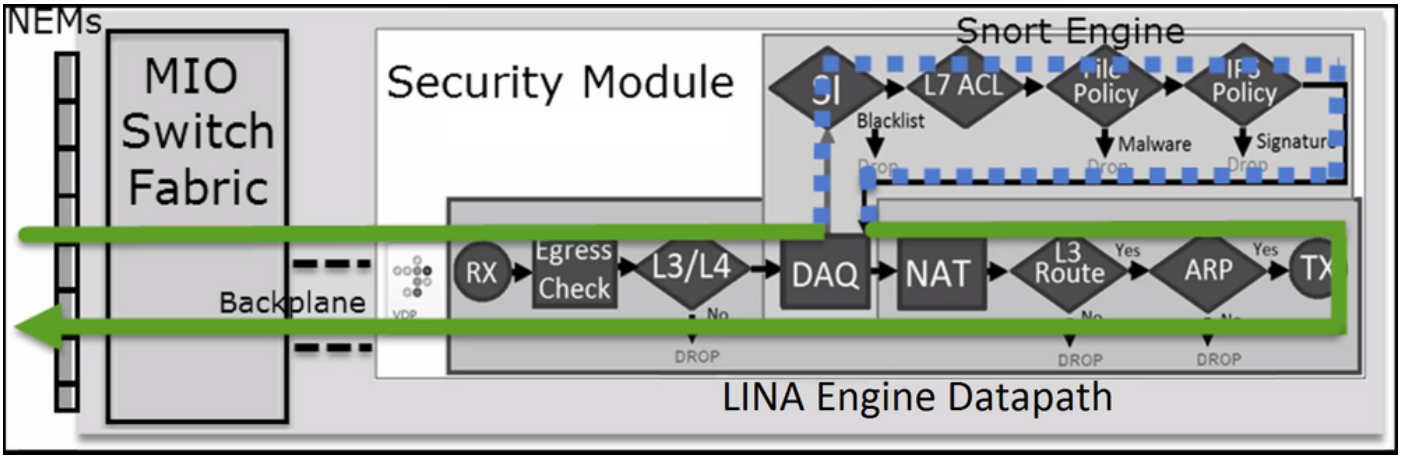
```
firepower# show capture CAPI packet-number 4 trace

441 packets captured

   4: 10:34:02.741523       802.1Q vlan#202 P0 192.168.10.50.42158 > 192.168.11.50.80: P
164375589:164375738(149) ack 3008397532 win 229 <nop,nop,timestamp 3789654678 57697031>
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found flow with id 1254, using existing flow

Phase: 4
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (fast-forward) fast forward this flow

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
Action: allow


1 packet shown
```

Les statistiques du renifleur confirment ceci :

```
firepower# show snort statistics

Packet Counters:
  Passed Packets                                         2
  Blocked Packets                                        0
  Injected Packets                                       0
  Packets bypassed (Snort Down)                          0
  Packets bypassed (Snort Busy)                          0

Flow Counters:
  Fast-Forwarded Flows                                   1
  Blacklisted Flows                                      0
```

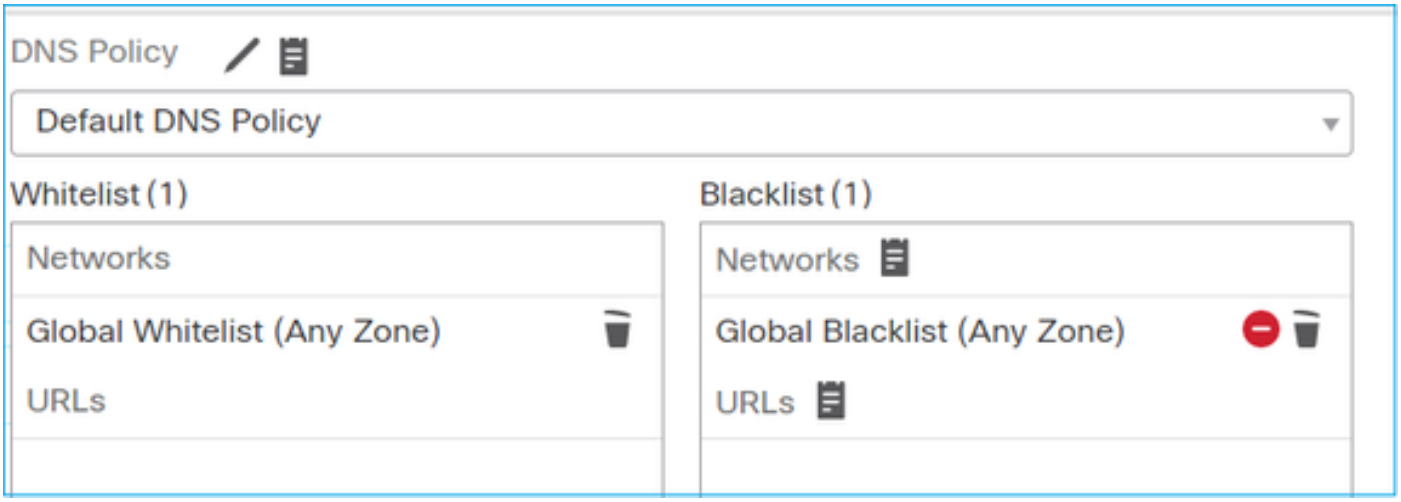
```
Miscellaneous Counters:
  Start-of-Flow events                                                    0
  End-of-Flow events                                                      1
  Denied flow events                                                      0
  Frames forwarded to Snort before drop                                   0
  Inject packets dropped                                                  0
```

Flux de paquets avec la règle Trust (confiance). Quelques paquets sont inspectés par le renifleur et le reste par LINA :



Scénario 2. Action de confiance ACP (sans SI, QoS et politique d'identité)

Si vous souhaitez que le FTD applique des contrôles de sécurité adaptative (SI) à tous les flux, SI est déjà activé au niveau ACP et vous pouvez spécifier les sources SI (TALOS, flux, listes, etc.). D'un autre côté, si vous souhaitez les désactiver, vous désactivez Security Intelligence pour les réseaux dans le monde conformément à la politique de contrôle d'accès, Security Intelligence pour l'URL et Security Intelligence pour le DNS. Security Intelligence pour les réseaux et l'URL sont désactivés, comme le montre l'image :



Dans ce cas, la règle Trust (confiance) est déployée dans LINA en tant que trust :

```
> show access-list
...
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L4 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced trust ip host 192.168.1.40 host 192.168.2.40 rule-id
268435461 event-log flow-end (hitcnt=0) 0x5c1346d6
```

Note: À partir de la section 6.2.2, FTD prend en charge TID. Cisco TID fonctionne de manière similaire à Security Intelligence, mais si cette dernière est désactivée, elle ne « force » pas la redirection de paquets vers le moteur du renifleur pour l'inspection de Cisco TID.

Vérifiez le comportement

Lancez une session HTTP de l'hôte-A (192.168.1.40) à l'hôte-B (192.168.2.40). Comme il s'agit d'un FP4100 et qu'il prend en charge le déchargement de flux dans le matériel, ces choses se produisent :

- Quelques paquets sont acheminés par le moteur FTD LINA, et le reste du flux est transféré vers SmartNIC (accélérateur matériel)
- Aucun paquet n'est transféré au moteur Snort

La table de connexion FTD LINA affiche l'indicateur '**o**' ce qui signifie que le flux a été déchargé vers le matériel. En outre, notez l'absence de la mention «**N**'. Cela signifie essentiellement « no Snort redirection » (pas de redirection vers le renifleur) :

```
firepower# show conn
1 in use, 15 most used

TCP OUTSIDE  192.168.2.40:80 INSIDE  192.168.1.40:32809, idle 0:00:00, bytes 949584, flags UIOo
```

Les statistiques du renifleur affichent uniquement les événements de journalisation au début et à la fin de la session :

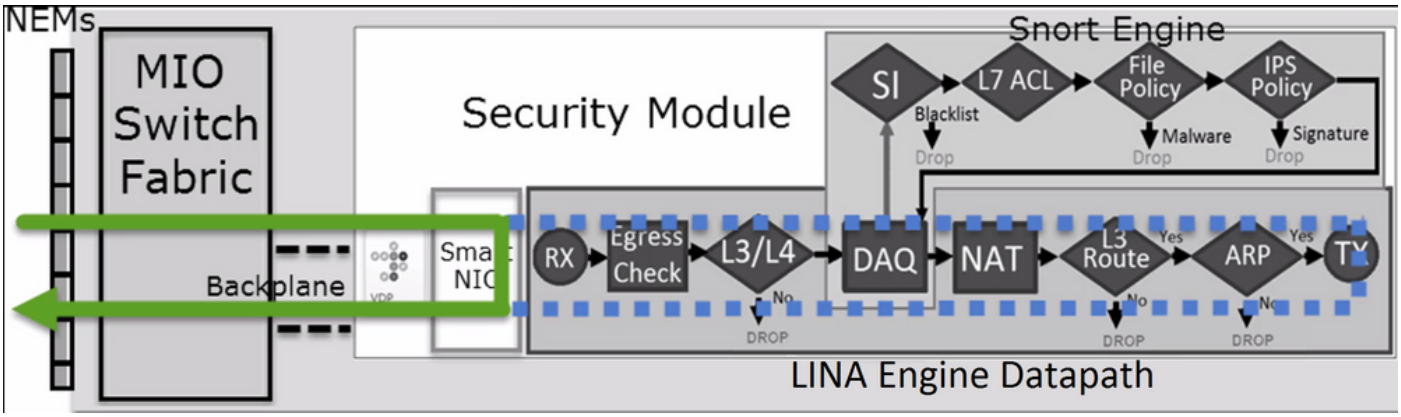
```
firepower# show snort statistics

Packet Counters:
  Passed Packets                                   0
  Blocked Packets                                  0
  Injected Packets                                 0
  Packets bypassed (Snort Down)                    0
  Packets bypassed (Snort Busy)                    0

Flow Counters:
  Fast-Forwarded Flows                             0
  Blacklisted Flows                                0

Miscellaneous Counters:
  Start-of-Flow events                             1
  End-of-Flow events                               1
```

Les journaux FTD LINA montrent que pour chaque session, deux flux (un par direction) ont été transférés vers le matériel :

```
Sep 27 2017 20:16:05: %ASA-7-609001: Built local-host INSIDE:192.168.1.40
Sep 27 2017 20:16:05: %ASA-6-302013: Built inbound TCP connection 25384 for
INSIDE:192.168.1.40/32809 (192.168.1.40/32809) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Sep 27 2017 20:16:05: %ASA-6-805001: Offloaded TCP Flow for connection 25384 from
INSIDE:192.168.1.40/32809 (192.168.1.40/32809) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
```

```
Sep 27 2017 20:16:05: %ASA-6-805001: Offloaded TCP Flow for connection 25384 from
OUTSIDE:192.168.2.40/80 (192.168.2.40/80) to INSIDE:192.168.1.40/32809 (192.168.1.40/32809)
Sep 27 2017 20:16:05: %ASA-6-805002: TCP Flow is no longer offloaded for connection 25384 from
OUTSIDE:192.168.2.40/80 (192.168.2.40/80) to INSIDE:192.168.1.40/32809 (192.168.1.40/32809)
Sep 27 2017 20:16:05: %ASA-6-805002: TCP Flow is no longer offloaded for connection 25384 from
INSIDE:192.168.1.40/32809 (192.168.1.40/32809) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Sep 27 2017 20:16:05: %ASA-6-302014: Teardown TCP connection 25384 for INSIDE:192.168.1.40/32809
to OUTSIDE:192.168.2.40/80 duration 0:00:00 bytes 1055048 TCP FINs
Sep 27 2017 20:16:05: %ASA-7-609002: Teardown local-host INSIDE:192.168.1.40 duration 0:00:00
```

Flux de paquets avec la règle de confiance déployée comme **trust** dans LINA. Quelques paquets sont inspectés par LINA, le reste est déchargé sur SmartNIC (FP4100/FP9300) :

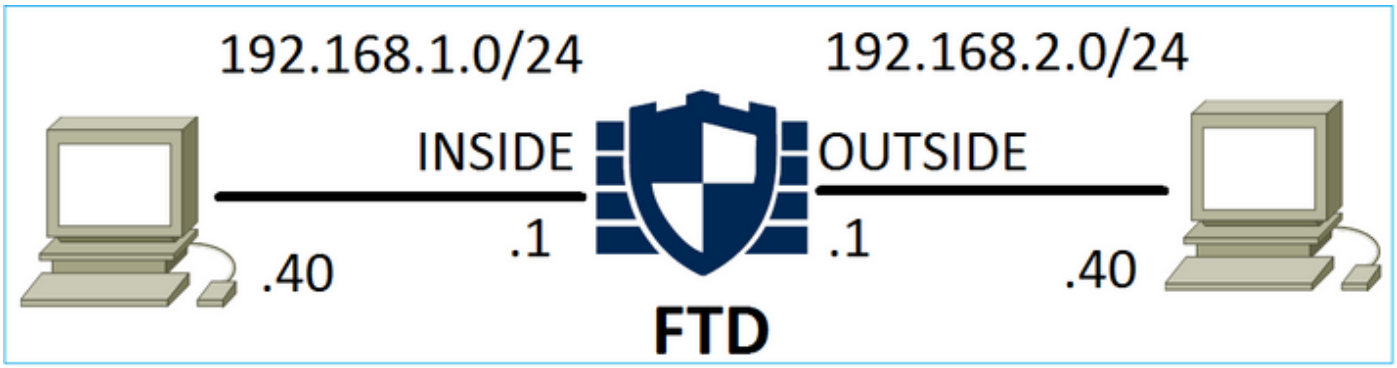


Scénarios :

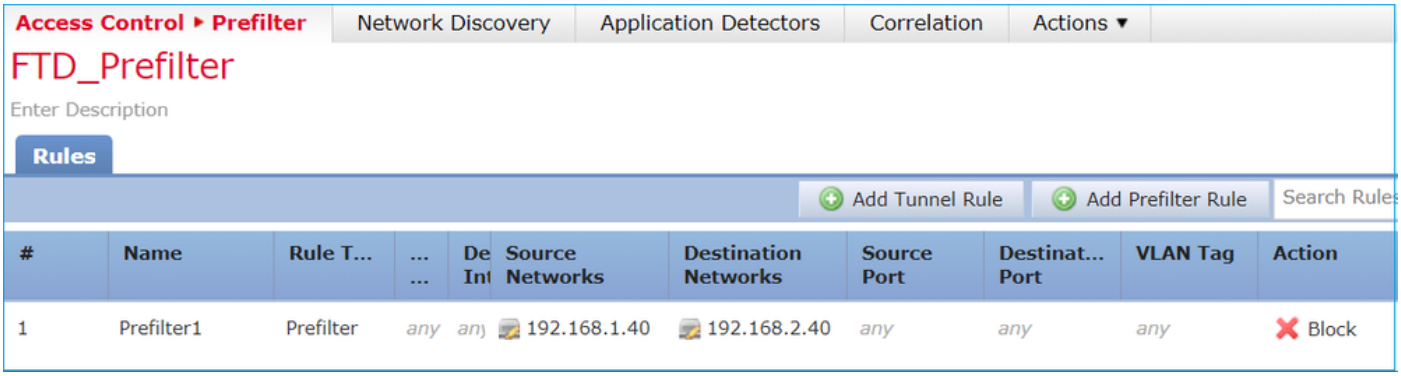
- Vous devez utiliser **Trust** lorsque vous souhaitez que seuls quelques paquets soient vérifiés par le moteur Snort (par exemple, détection d'application, vérification SI) et que le reste du flux soit déchargé vers le moteur LINA
- Si vous utilisez FTD sur FP4100/9300 et que vous voulez que le flux contourne complètement l'inspection Snort, alors considérez la règle de préfiltrage avec **Fastpath** action (voir la section associée dans ce document)

Action Prefilter Policy Block (blocage de la politique de préfiltre)

Considérez la topologie comme le montre l'image :



Tenez également compte de la politique, comme le montre l'image :



Voici la stratégie déployée dans le moteur FTD Snort (fichier ngfw.rules) :

```
# Start of tunnel and priority rules.
# These rules are evaluated by LINA. Only tunnel tags are used from the matched rule id.
268437506 deny any 192.168.1.40 32 any any 192.168.2.40 32 any any any  (tunnel -1
```

Dans LINA :

```
access-list CSM_FW_ACL_ line 1 remark rule-id 268437506: PREFILTER POLICY: FTD_Prefilter
access-list CSM_FW_ACL_ line 2 remark rule-id 268437506: RULE: Prefilter1
access-list CSM_FW_ACL_ line 3 advanced deny ip host 192.168.1.40 host 192.168.2.40 rule-id
268437506 event-log flow-start (hitcnt=0) 0x76476240
```

Lorsque vous tracez un paquet virtuel, cela indique que le paquet est abandonné par LINA et n'est jamais transmis au renifleur :

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
…
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip host 192.168.1.40 host 192.168.2.40 rule-id 268437506
event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268437506: PREFILTER POLICY: FTD_Prefilter
access-list CSM_FW_ACL_ remark rule-id 268437506: RULE: Prefilter1
Additional Information:

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

Les statistiques du renifleur montrent :

```
firepower# show snort statistics
```

```
Packet Counters:
  Passed Packets                                         0
  Blocked Packets                                        0
  Injected Packets                                       0
  Packets bypassed (Snort Down)                          0
  Packets bypassed (Snort Busy)                          0

Flow Counters:
  Fast-Forwarded Flows                                   0
  Blacklisted Flows                                      0

Miscellaneous Counters:
  Start-of-Flow events                                   0
  End-of-Flow events                                     0
  Denied flow events                                     1
```

La politique de contrôle d'accès de LINA affiche :

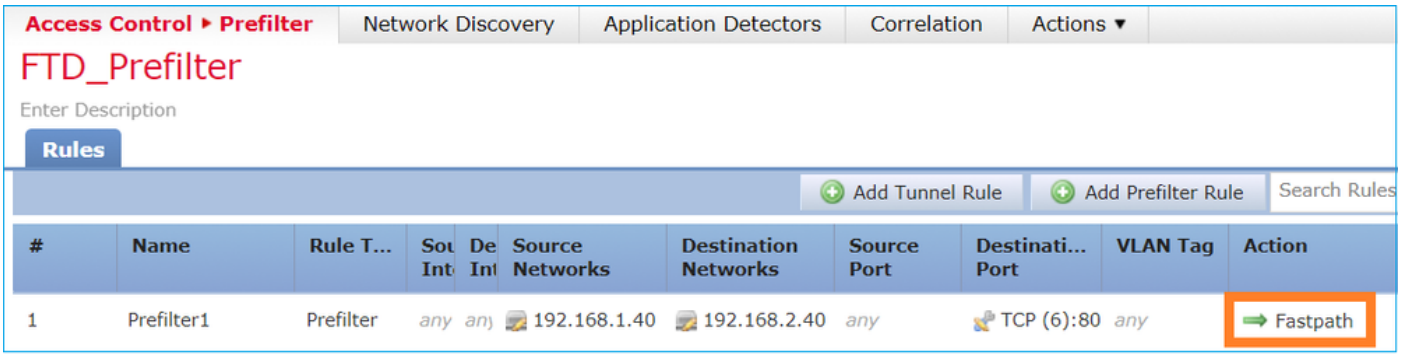
```
firepower# show asp drop

Frame drop:
  Flow is denied by configured rule (acl-drop)               1
```

Scénarios :

Vous pouvez utiliser une règle de blocage de préfiltre lorsque vous souhaitez bloquer le trafic en fonction des conditions L3/L4 et sans avoir à effectuer d'inspection Snort du trafic.

Action Prefilter Policy Fastpath (Fastpath pour la politique de préfiltre)

Tenez compte de la règle de politique de préfiltre, comme le montre l'image :



Voici la stratégie déployée dans le moteur FTD Snort :

```
268437506 fastpath any any any any any any any any (log dcforward flowend) (tunnel -1)
```

Dans FTD LINA :

```
access-list CSM_FW_ACL_ line 1 remark rule-id 268437506: PREFILTER POLICY: FTD_Prefilter
access-list CSM_FW_ACL_ line 2 remark rule-id 268437506: RULE: Prefilter1
access-list CSM_FW_ACL_ line 3 advanced trust tcp host 192.168.1.40 host 192.168.2.40 eq www
rule-id 268437506 event-log flow-end (hitcnt=0) 0xf3410b6f
```

Vérifiez le comportement

Lorsque l'hôte A (192.168.1.40) tente d'ouvrir une session HTTP vers l'hôte B (192.168.2.40), quelques paquets passent par LINA, et le reste est déchargé vers SmartNIC. In this case **system support trace** avec **firewall-engine-debug** affiche les résultats activés :

```
> system support trace

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.1.40
Please specify a client port:
Please specify a server IP address: 192.168.2.40
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages

192.168.1.40-32840 > 192.168.2.40-80 6 AS 1 I 8 Got end of flow event from hardware with flags
04000000
```

Les journaux LINA indiquent le flux déchargé :

```
Oct 01 2017 14:36:51: %ASA-7-609001: Built local-host INSIDE:192.168.1.40
Oct 01 2017 14:36:51: %ASA-7-609001: Built local-host OUTSIDE:192.168.2.40
Oct 01 2017 14:36:51: %ASA-6-302013: Built inbound TCP connection 966 for
INSIDE:192.168.1.40/32840 (192.168.1.40/32840) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Oct 01 2017 14:36:51: %ASA-6-805001: Offloaded TCP Flow for connection 966 from
INSIDE:192.168.1.40/32840 (192.168.1.40/32840) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Oct 01 2017 14:36:51: %ASA-6-805001: Offloaded TCP Flow for connection 966 from
OUTSIDE:192.168.2.40/80 (192.168.2.40/80) to INSIDE:192.168.1.40/32840 (192.168.1.40/32840)
```

Les captures LINA indiquent que 8 paquets transitent par :

```
firepower# show capture
capture CAPI type raw-data buffer 33554432 trace trace-count 100 interface INSIDE [Capturing -
3908 bytes]
  match ip host 192.168.1.40 host 192.168.2.40
capture CAPO type raw-data buffer 33554432 trace trace-count 100 interface OUTSIDE [Capturing -
3908 bytes]
  match ip host 192.168.1.40 host 192.168.2.40


firepower# show capture CAPI

8 packets captured

   1: 14:45:32.700021  192.168.1.40.32842 > 192.168.2.40.80: S 3195173118:3195173118(0) win 2920
<mss 1460,sackOK,timestamp 332569060 0>
   2: 14:45:32.700372  192.168.2.40.80 > 192.168.1.40.32842: S 184794124:184794124(0) ack
3195173119 win 2896 <mss 1380,sackOK,timestamp 332567732 332569060>
   3: 14:45:32.700540  192.168.1.40.32842 > 192.168.2.40.80: P 3195173119:3195173317(198) ack
184794125 win 2920 <nop,nop,timestamp 332569060 332567732>
   4: 14:45:32.700876  192.168.2.40.80 > 192.168.1.40.32842: . 184794125:184795493(1368) ack
3195173317 win 2698 <nop,nop,timestamp 332567733 332569060>
   5: 14:45:32.700922  192.168.2.40.80 > 192.168.1.40.32842: P 184795493:184796861(1368) ack
```

```
3195173317 win 2698 <nop,nop,timestamp 332567733 332569060>
   6: 14:45:32.701425  192.168.2.40.80 > 192.168.1.40.32842: FP 184810541:184810851(310) ack
3195173317 win 2698 <nop,nop,timestamp 332567733 332569061>
   7: 14:45:32.701532  192.168.1.40.32842 > 192.168.2.40.80: F 3195173317:3195173317(0) ack
184810852 win 2736 <nop,nop,timestamp 332569061 332567733>
   8: 14:45:32.701639  192.168.2.40.80 > 192.168.1.40.32842: . ack 3195173318 win 2697
<nop,nop,timestamp 332567734 332569061>
```

Les statistiques de flux de déchargement de Cisco FTD indiquent 22 paquets déchargés sur le matériel :

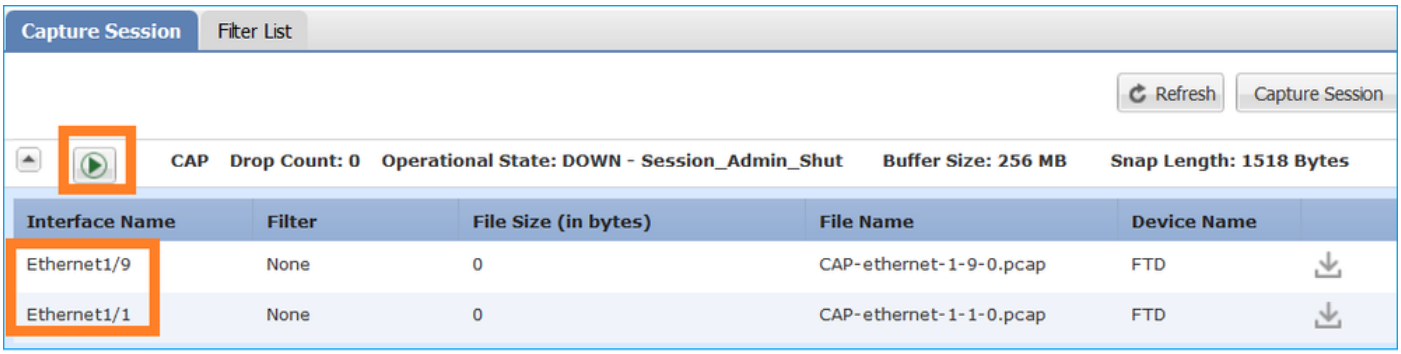
```
firepower# show flow-offload statistics
 Packet stats of port : 0
        Tx Packet count                 :              22
        Rx Packet count                 :              22
        Dropped Packet count            :               0
        VNIC transmitted packet         :              22
        VNIC transmitted bytes          :           15308
        VNIC Dropped packets            :               0
        VNIC erroneous received         :               0
        VNIC CRC errors                 :               0
        VNIC transmit failed            :               0
        VNIC multicast received         :               0
```

Vous pouvez également utiliser la **show flow-offload flow** pour afficher des informations supplémentaires relatives aux flux déchargés. Voici un exemple :

```
firepower# show flow-offload flow
Total offloaded flow stats: 2 in use, 4 most used, 20% offloaded, 0 collisions
TCP intfc 103 src 192.168.1.40:39301 dest 192.168.2.40:20, static, timestamp 616063741, packets
33240, bytes 2326800
TCP intfc 104 src 192.168.2.40:20 dest 192.168.1.40:39301, static, timestamp 616063760, packets
249140, bytes 358263320
firepower# show conn
5 in use, 5 most used
Inspect Snort:
       preserve-connection: 1 enabled, 0 in effect, 4 most enabled, 0 most in effect

TCP OUTSIDE  192.168.2.40:21 INSIDE  192.168.1.40:40988, idle 0:00:00, bytes 723, flags UIO
TCP OUTSIDE  192.168.2.40:21 INSIDE  192.168.1.40:40980, idle 0:02:40, bytes 1086, flags UIO
TCP OUTSIDE  192.168.2.40:80 INSIDE  192.168.1.40:49442, idle 0:00:00, bytes 86348310, flags UIO
N1
TCP OUTSIDE  192.168.2.40:20 INSIDE  192.168.1.40:39301, idle 0:00:00, bytes 485268628, flags Uo
<- offloaded flow
TCP OUTSIDE  192.168.2.40:20 INSIDE  192.168.1.40:34713, idle 0:02:40, bytes 821799360, flags
UFRIO
```

- Le pourcentage est basé sur le '**show conn**' résultat. Par exemple, si 5 cons au total passent par le moteur FTD LINA et que 1 d'entre eux est déchargé, alors 20 % est déclaré comme déchargé
- La limite maximale de sessions déchargées dépend de la version du logiciel (par exemple, ASA 9.8.3 et FTD 6.2.3 prennent en charge 4 millions de flux déchargés bidirectionnels (ou 8 millions de flux unidirectionnels))
- Si le nombre de flux déchargés atteint la limite (par exemple 4 millions de flux bidirectionnels), aucune nouvelle connexion n'est déchargée tant que les connexions en cours ne sont pas supprimées de la table déchargée

Afin de voir tous les paquets sur FP4100/9300 qui passent par Cisco FTD (déchargé + LINA), il est nécessaire d'activer la capture au niveau du châssis, comme le montre l'image :



La capture du fond de panier du châssis indique les deux directions. En raison de l'architecture de capture FXOS (deux points par direction), chaque paquet est présenté **deux fois**, comme le montre l'image :

Statistiques sur les paquets :

- Total des paquets passant par Cisco FTD : 30
- Paquets passant par FTD LINA : 8
- Paquets déchargés vers l'accélérateur SmartNIC HW : 22

Dans le cas d'une plate-forme différente de FP4100/FP9300, tous les paquets sont traités par le moteur LINA puisque le déchargement de flux n'est pas pris en charge (notez l'absence de l'indicateur **o**) :

```
FP2100-6# show conn addr 192.168.1.40
33 in use, 123 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 2 most enabled, 0 most in effect

TCP OUTSIDE  192.168.2.40:80 INSIDE  192.168.1.40:50890, idle 0:00:09, bytes 175, flags UxIO
```

Les syslogs LINA affichent uniquement les événements de mise à disposition et de fin de connexion :

```
FP2100-6# show log | i 192.168.2.40
Jun 21 2020 14:29:44: %FTD-6-302013: Built inbound TCP connection 6914 for
INSIDE:192.168.1.40/50900 (192.168.11.101/50900) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Jun 21 2020 14:30:30: %FTD-6-302014: Teardown TCP connection 6914 for INSIDE:192.168.1.40/50900
to OUTSIDE:192.168.2.40/80 duration 0:00:46 bytes 565 TCP FINs from OUTSIDE
```

Scénarios :

- Utilisation **Prefilter Fastpath** lorsque vous souhaitez contourner complètement l'inspection Snort. Vous devez généralement faire cela pour les gros flux de confiance, comme les sauvegardes, les transferts de base de données, etc.
- Sur les appliances FP4100/9300, **Fastpath** déclenche le déchargement de flux et seuls quelques paquets passent par le moteur FTD LINA. Le reste est géré par SmartNIC, ce qui réduit la latence

Action Prefilter Policy Fastpath (Fastpath pour la politique de préfiltre) (ensemble en ligne)

Dans le cas où une action FastPath de stratégie de préfiltrage est appliquée au trafic qui passe par un ensemble en ligne (interfaces NGIPS), ces points doivent être pris en considération :

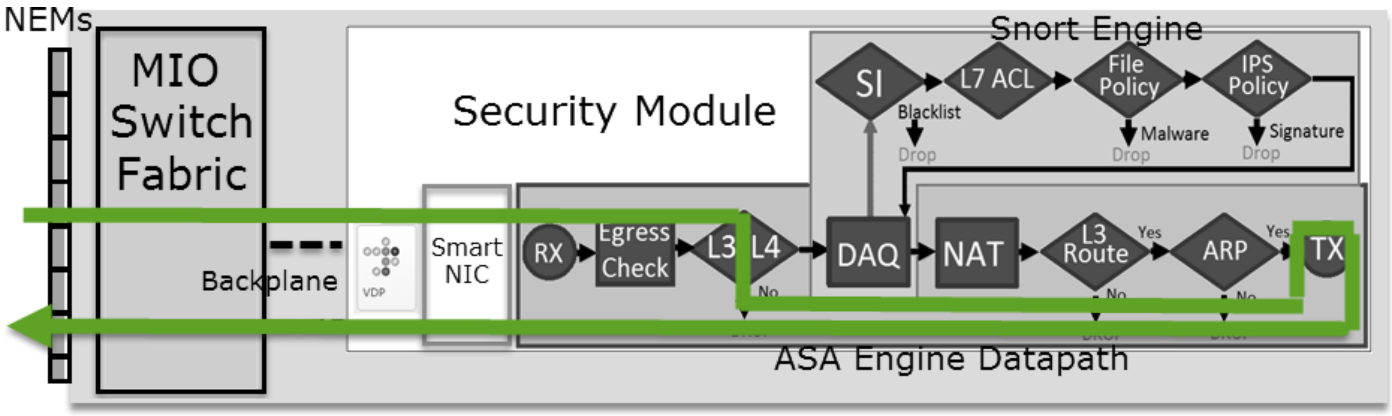
- La règle est appliquée au moteur LINA en tant que **trust** action
- Le flux n'est pas contrôlé par le moteur du renifleur
- Le déchargement de flux (accélération matérielle) ne se produit pas, car le déchargement de flux ne s'applique pas aux interfaces NGIPS

Voici un exemple de suivi de paquet dans le cas d'une action de préfiltrage FastPath appliquée à un jeu en ligne :

```
firepower# packet-tracer input inside tcp 192.168.1.40 12345 192.168.1.50 80 detailed

Phase: 1
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied
Forward Flow based lookup yields rule:
in id=0x2ad7ac48b330, priority=501, domain=ips-mode, deny=false
hits=2, user_data=0x2ad80d54abd0, cs_id=0x0, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=inside, output_ifc=any

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced trust ip object 192.168.1.0 object 192.168.1.0 rule-id
268438531 event-log flow-end
access-list CSM_FW_ACL_ remark rule-id 268438531: PREFILTER POLICY: PF1
access-list CSM_FW_ACL_ remark rule-id 268438531: RULE: 1
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ad9f9f8a7f0, priority=12, domain=permit, trust
hits=1, user_data=0x2ad9b23c5d40, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=192.168.1.0, mask=255.255.255.0, port=0, tag=any, ifc=any
dst ip/id=192.168.1.0, mask=255.255.255.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 3
Type: NGIPS-EGRESS-INTERFACE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
Ingress interface inside is in NGIPS inline mode.
Egress interface outside is determined by inline-set configuration

Phase: 4
Type: FLOW-CREATION
Subtype:
Result: ALLOW
```

```
Config:
Additional Information:
New flow created with id 7, packet dispatched to next module
Module information for forward flow ...
snp_fp_ips_tcp_state_track_lite
snp_fp_ips_mode_adj
snp_fp_tracer_drop
snp_ifc_stat

Module information for reverse flow ...
snp_fp_ips_tcp_state_track_lite
snp_fp_ips_mode_adj
snp_fp_tracer_drop
snp_ifc_stat

Result:
input-interface: inside
input-status: up
input-line-status: up
Action: allow
```

Voici la représentation visuelle du chemin du paquet :



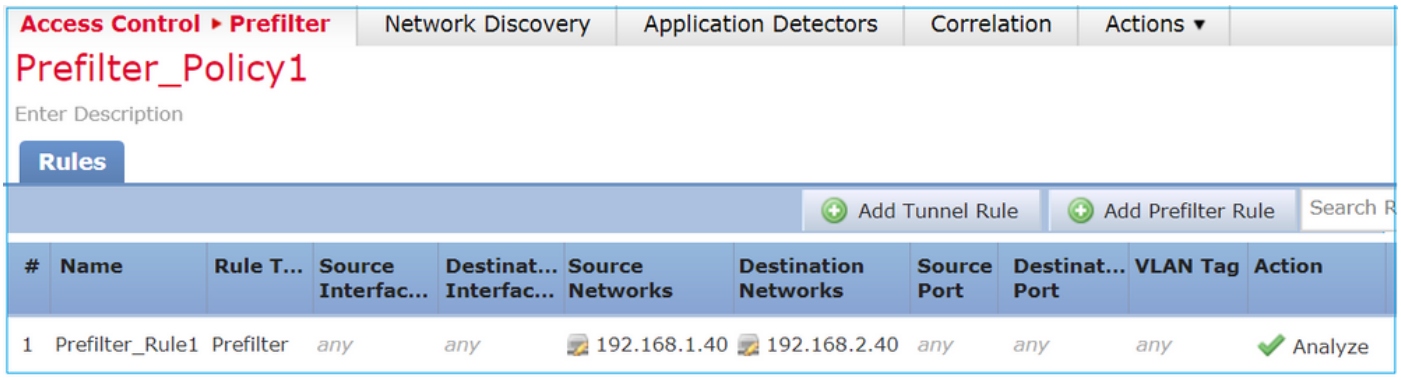
Action Prefilter Policy Fastpath (Fastpath pour la politique de préfiltre) (ensemble en ligne avec dérivateur)

Identique au cas d'ensemble en ligne

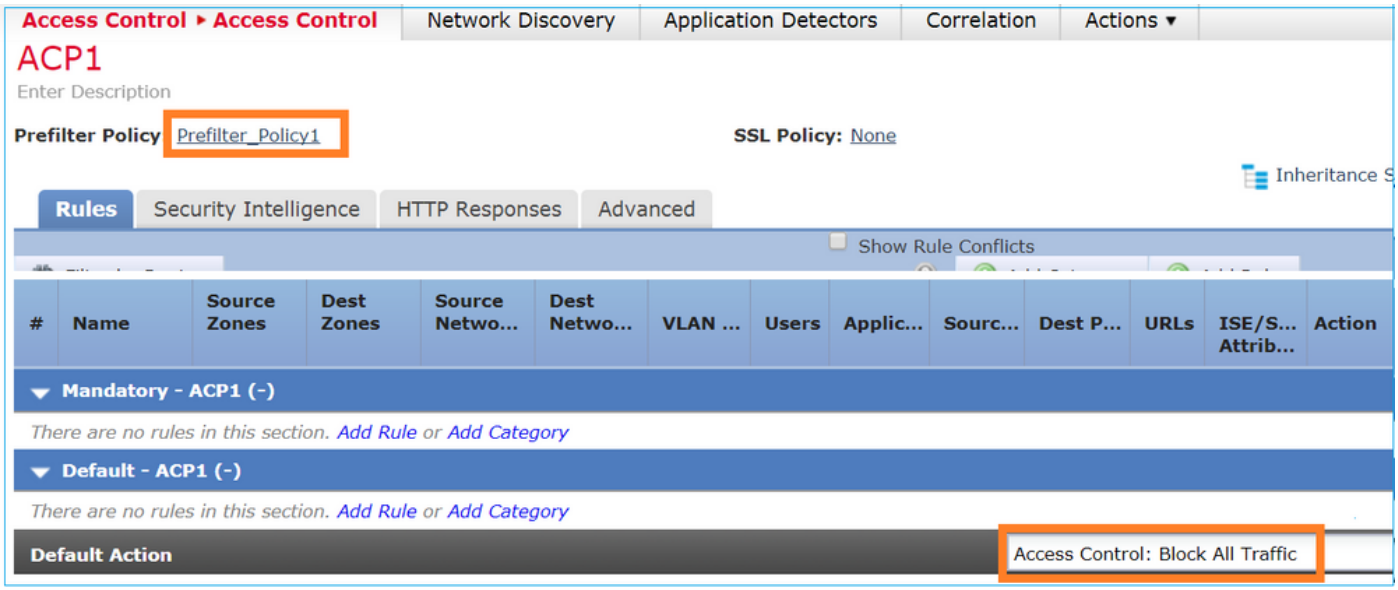
Action Prefilter Policy Analyze (analyse de la politique de préfiltre)

Scénario 1. Préfiltrer l'analyse avec la règle de blocage ACP

Tenez compte de la règle Prefilter Policy (politique de préfiltre) qui contient une règle Analyze (analyse), comme le montre l'image :



L'ACP contient uniquement la règle par défaut définie sur **Block All Traffic** comme le montre l'image :



Voici la stratégie déployée dans le moteur FTD Snort (fichier ngfw.rules) :

```
# Start of tunnel and priority rules.
# These rules are evaluated by LINA. Only tunnel tags are used from the matched rule id.
268435460 allow any 192.168.1.40 32 any any 192.168.2.40 32 any any any  (tunnel -1)
268435459 allow any any  1025-65535 any any  3544 any 17  (tunnel -1)
268435459 allow any any  3544 any any  1025-65535 any 17  (tunnel -1)
268435459 allow any any  any any any  any any 47  (tunnel -1)
268435459 allow any any  any any any  any any 41  (tunnel -1)
268435459 allow any any  any any any  any any 4  (tunnel -1)
# End of tunnel and priority rules.
# Start of AC rule.
268435458 deny any any  any any any  any any any  (log dcforward flowstart)
# End of AC rule.
```

Voici la politique déployée dans le moteur FTD LINA :

```
access-list CSM_FW_ACL_ line 3 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435460 (hitcnt=0) 0xb788b786
```

Vérifiez le comportement

Packet-Tracer indique que le paquet est autorisé par LINA, est transféré au moteur Snort (en raison de **permit**) et Snort Engine renvoie une **Block** verdict, car l'action par défaut d'AC correspond.

> **Note**: Le renifleur n'évalue pas le trafic en fonction des règles du tunnel

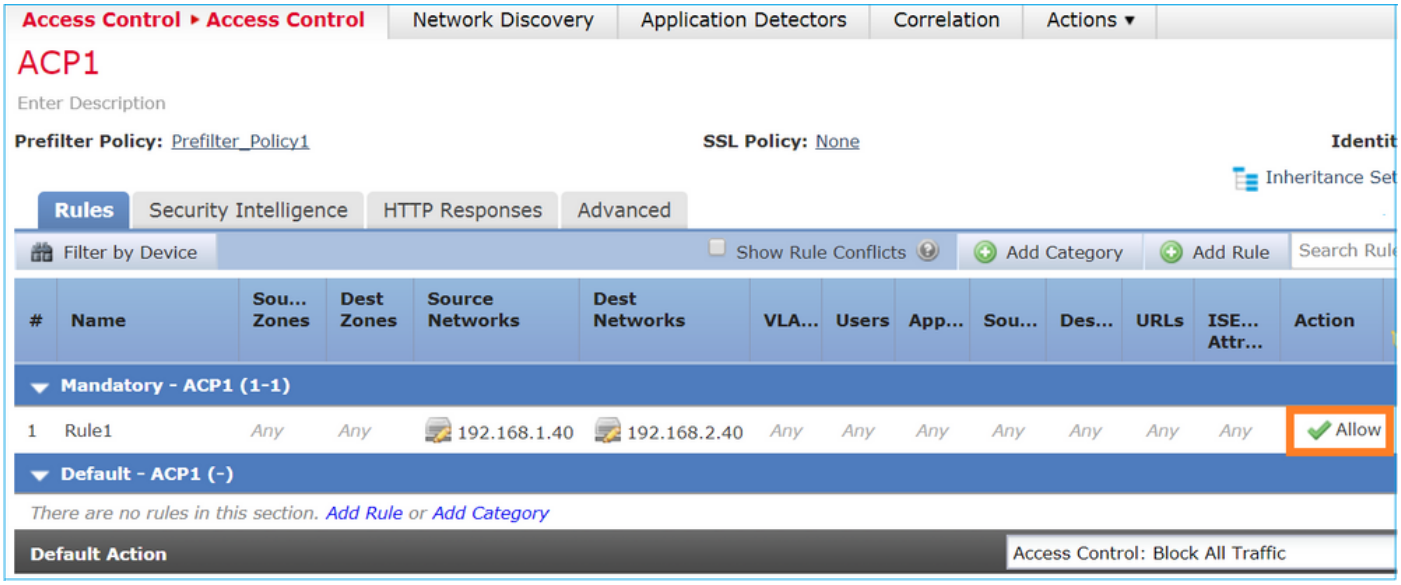
Lorsque vous tracez un paquet, il révèle la même chose :

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
```

```
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will be reached

…
Phase: 14
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: ICMP
AppID: service ICMP (3501), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 8, icmpCode 0
Firewall: block rule, id 268435458, drop
Snort: processed decoder alerts or actions queue, drop
NAP id 1, IPS id 0, Verdict BLOCKLIST, Blocked by Firewall
Snort Verdict: (block-list) block list this flow

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: drop
Drop-reason: (firewall) Blocked by the firewall preprocessor
```

Scénario 2. Préfiltrer l'analyse avec la règle d'autorisation ACP

Si l'objectif est de permettre au paquet de traverser Cisco FTD, il est nécessaire d'ajouter une règle dans la politique de contrôle d'accès. L'action peut être Autoriser ou Approuver selon l'objectif (par exemple, si vous souhaitez appliquer une inspection de couche 7, vous devez utiliser **Allow** action) comme l'illustre l'image :



La politique déployée dans le moteur FTD du renifleur :

```
# Start of AC rule.
268435461 allow any 192.168.1.40 32 any any 192.168.2.40 32 any any any
268435458 deny any any  any any any  any any any  (log dcforward flowstart)
# End of AC rule.
```

Dans le moteur LINA :

```
access-list CSM_FW_ACL_ line 3 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435460 (hitcnt=1) 0xb788b786
```

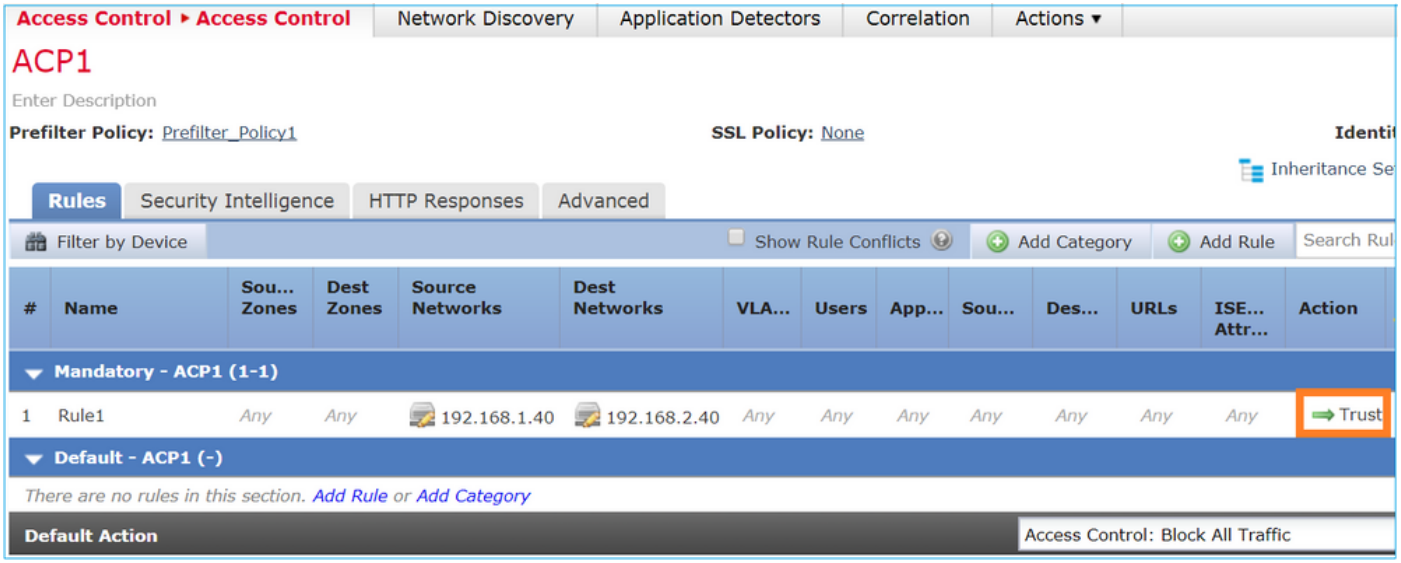
Vérifiez le comportement

Packet-Tracer indique que le paquet correspond à la règle **268435460** dans LINA et **268435461** dans le moteur Snort :

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will be reached
…
Phase: 14
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: ICMP
AppID: service ICMP (3501), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 8, icmpCode 0
Firewall: allow rule, id 268435461, allow
NAP id 1, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet
…
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow
```

Scénario 3. Préfiltrer l'analyse avec la règle d'approbation ACP

Dans le cas où la politique de contrôle d'accès contient une règle Trust (confiance), c'est ce que vous avez, comme le montre l'image :



Renifleur :

```
# Start of AC rule.
268435461 fastpath any 192.168.1.40 32 any any 192.168.2.40 32 any any any
268435458 deny any any  any any any  any any any  (log dcforward flowstart)
# End of AC rule.
```

LINA :

```
access-list CSM_FW_ACL_ line 3 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435460 (hitcnt=2) 0xb788b786
```

N'oubliez pas que puisque l'interface utilisateur est activée par défaut, la règle d'approbation est déployée en tant que **permit** sur LINA afin qu'au moins quelques paquets soient redirigés vers le moteur Snort pour inspection.

Vérifiez le comportement

Packet-tracer montre que le moteur Snort Autorise répertorie le paquet et décharge essentiellement le flux de repos vers LINA :

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will be reached
…
Phase: 14
```

```
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: ICMP
AppID: service ICMP (3501), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 8, icmpCode 0
Firewall: trust/fastpath rule, id 268435461, allow
NAP id 1, IPS id 0, Verdict PERMITLIST
Snort Verdict: (fast-forward) fast forward this flow
…
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow
```

Scénario 4. Préfiltrer l'analyse avec la règle d'approbation ACP

Dans ce scénario, Security Intelligence a été désactivée manuellement.

La règle est déployée dans le renifleur comme suit :

```
# Start of AC rule.
268435461 fastpath any 192.168.1.40 32 any any 192.168.2.40 32 any any any
268435458 deny any any  any any any  any any any  (log dcforward flowstart)
# End of AC rule.
```

Dans LINA, la règle est déployée en tant que Trust (confiance). Un paquet qui correspond à la règle d'autorisation (voir le nombre de succès ACE) qui est déployé en raison de la règle Analyze Prefilter et le paquet est inspecté par le moteur Snort :

```
access-list CSM_FW_ACL_ line 3 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435460 (hitcnt=3) 0xb788b786
...
access-list CSM_FW_ACL_ line 13 advanced trust ip host 192.168.1.40 host 192.168.2.40 rule-id
268435461 event-log flow-end (hitcnt=0) 0x5c1346d6
...
access-list CSM_FW_ACL_ line 16 advanced deny ip any any rule-id 268435458 event-log flow-start
(hitcnt=0) 0x97aa021a
```

Vérifiez le comportement

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
```

```
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will be reached
...
Phase: 14
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: ICMP
AppID: service ICMP (3501), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 8, icmpCode 0
Firewall: trust/fastpath rule, id 268435461, allow
NAP id 1, IPS id 0, Verdict PERMITLIST
Snort Verdict: (fast-forward) fast forward this flow
…
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow
```

Points principaux

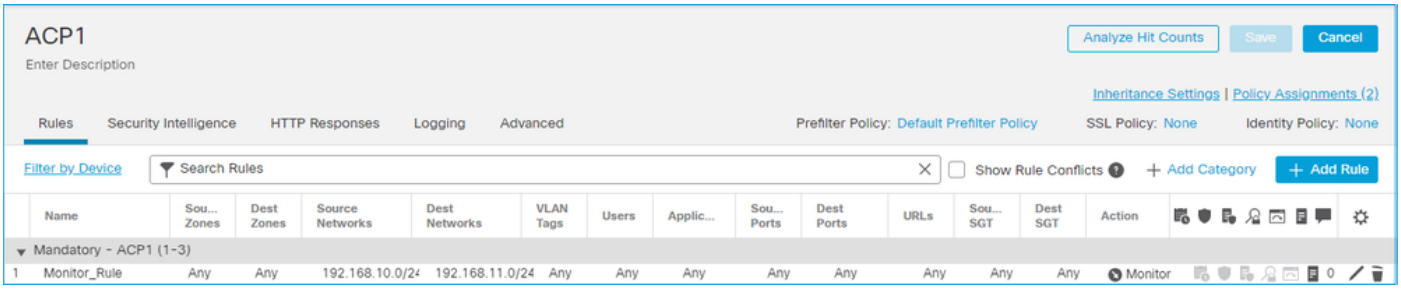
- Les **Analyze** L'action est déployée en tant que règle d'autorisation dans le moteur LINA. Cela a un effet sur le paquet à transmettre au moteur Snort pour inspection
- Les **Analyze** L'action ne déploie aucune règle dans le moteur Snort. Vous devez donc vous assurer de configurer une règle dans ACP correspondant dans Snort<
- Cela dépend de la règle ACP qui est déployée dans le moteur Snort (**block** vs **allow** vs **fastpath**) aucun ou tous ou quelques paquets sont autorisés par Snort

Scénarios :

- Un exemple d'utilisation de **Analyze** L'action est quand vous avez une règle Fastpath large dans la politique de préfiltrage et que vous voulez mettre quelques exceptions pour des flux spécifiques afin qu'ils soient inspectés par Snort

Action Monitor (surveillance) de la politique de contrôle d’accès

Une règle Monitor (surveillance) configurée sur l’interface utilisateur de Cisco FMC :



La règle de surveillance est déployée sur le moteur FTD LINA en tant que **permit** et au moteur Snort en tant que **audit** action.

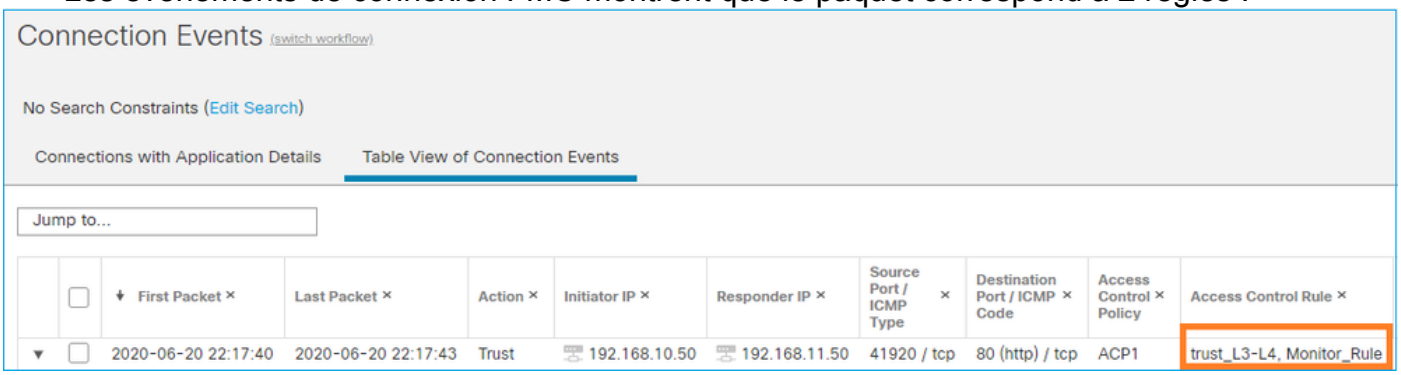
```
firepower# show access-list
…
access-list CSM_FW_ACL_ line 10 advanced permit ip 192.168.10.0 255.255.255.0 192.168.11.0
255.255.255.0 rule-id 268438863 (hitcnt=0) 0x61bbaf0c
```

La règle du renifleur :

```
admin@firepower:~$ cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules
…
# Start of AC rule.
268438863 audit any 192.168.10.0 24 any any 192.168.11.0 24 any any any (log dcforward flowend)
# End rule 268438863
```

Points principaux

- La règle de surveillance ne supprime ni n'autorise le trafic, mais génère un événement de connexion. Le paquet est vérifié par rapport aux règles suivantes et il est soit autorisé, soit abandonné
- Les événements de connexion FMC montrent que le paquet correspond à 2 règles :



System support trace Le résultat montre que les paquets correspondent aux deux règles :

```
> system support trace

Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.50
Please specify a client port:
Please specify a server IP address: 192.168.11.50
Please specify a server port:
Monitoring packet tracer and firewall debug messages
```

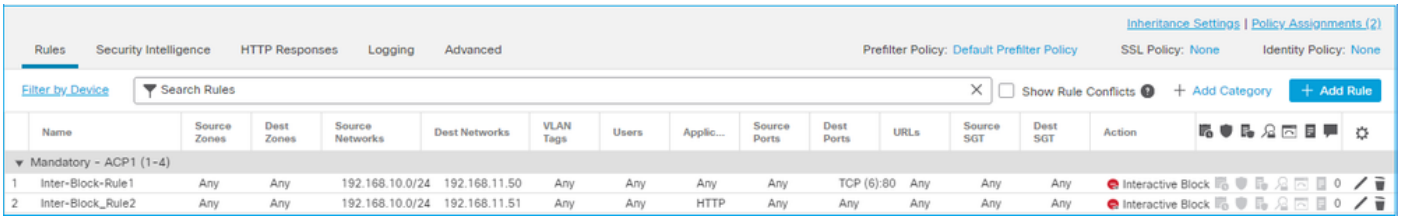
```
192.168.10.50-41922 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 419031630
192.168.10.50-41922 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.50-41922 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 new firewall session
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 Starting AC with minimum 2, 'Monitor_Rule',
and IPProto first with zone           s -1 -> -1, geo 0 -> 0, vlan 0, source sgt type: 0, source
sgt tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest sgt tag: 0,            svc 0, payload 0,
client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 match rule order 2, 'Monitor_Rule', action
Audit
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 match rule order 3, 'trust_L3-L4', action
Trust
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 MidRecovery data sent for rule id:
268438858,rule_action:3, rev id:1078           02206, rule_match flag:0x2
```

Scénarios :

Utilisé pour surveiller l'activité du réseau et générer un événement de connexion

Action Interactive Block (blocage interactif) de la politique de contrôle d'accès

Une règle Interactive Block (blocage interactif) configurée sur l'interface utilisateur de Cisco FMC :



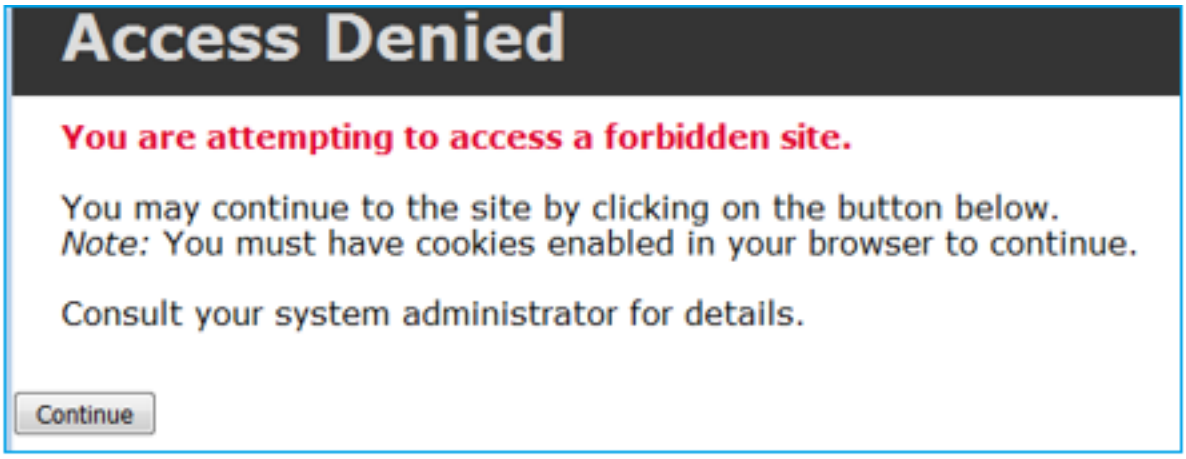
La règle de blocage interactif est déployée sur le moteur FTD LINA en tant que **permit** et au moteur Snort en tant que règle de contournement :

```
firepower# show access-list
…
access-list CSM_FW_ACL_ line 9 remark rule-id 268438864: L7 RULE: Inter-Block-Rule1
access-list CSM_FW_ACL_ line 10 advanced permit tcp 192.168.10.0 255.255.255.0 host
192.168.11.50 eq www rule-id 268438864 (hitcnt=3) 0xba785fc0
access-list CSM_FW_ACL_ line 11 remark rule-id 268438865: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268438865: L7 RULE: Inter-Block_Rule2
access-list CSM_FW_ACL_ line 13 advanced permit ip 192.168.10.0 255.255.255.0 host 192.168.11.51
rule-id 268438865 (hitcnt=0) 0x622350d0
```

Moteur du renifleur :

```
admin@firepower:~$ cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules
…
# Start of AC rule.
268438864 bypass any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6
# End rule 268438864
268438865 bypass any 192.168.10.0 24 any any 192.168.11.51 32 any any any (appid 676:1)
(ip_protos 6, 17)
# End rule 268438865
```

La règle Interactive Block (blocage interactif) invite l'utilisateur à interdire la destination



Par défaut, le pare-feu permet de contourner le blocage pendant 600 secondes :

Dans la **system support trace** résultat vous pouvez voir que le pare-feu bloque initialement le trafic et affiche la page de blocage :

```
> system support trace
…
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 983273680, ack
2014879580
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt
tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589,
misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 match rule order 2, 'Inter-Block-Rule1',
action Interactive
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 bypass action sending HTTP interactive
response of 1093 bytes
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive block rule, 'Inter-
Block-Rule1', drop
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions
queue, drop
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 deleting firewall session flags = 0x800,
fwFlags = 0x1002
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 22, NAP id 1, IPS id 0, Verdict
```

```
BLACKLIST
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 ===> Blocked by Firewall
Verdict reason is sent to DAQ
```

Une fois que l'utilisateur sélectionne **Continue** (ou actualise la page du navigateur) le débogage montre que les paquets sont autorisés par la même règle qui imite et **Allow** action :

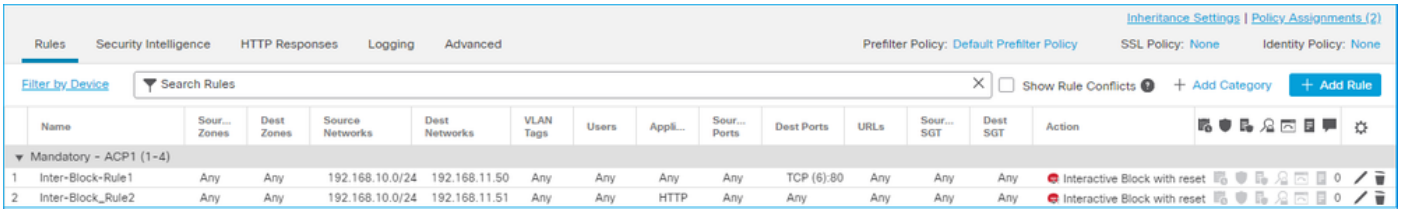
```
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 1357413630, ack
2607625293
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt
tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589,
misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 match rule order 2, 'Inter-Block-Rule1',
action Interactive
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 bypass action interactive bypass
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 allow action
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: allow rule, 'Inter-Block-Rule1',
allow
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive bypass rule, 'Inter-
Block-Rule1', allow
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 8, NAP id 1, IPS id 0, Verdict
PASS
```

Scénarios :

Afficher une page d’avertissement aux utilisateurs Web et leur donner la possibilité de continuer.

Action Interactive Block (blocage interactif) de la politique de contrôle d’accès avec réinitialisation

Une règle Interactive Block (blocage interactif) avec réinitialisation configurée sur l’interface utilisateur de Cisco FMC :



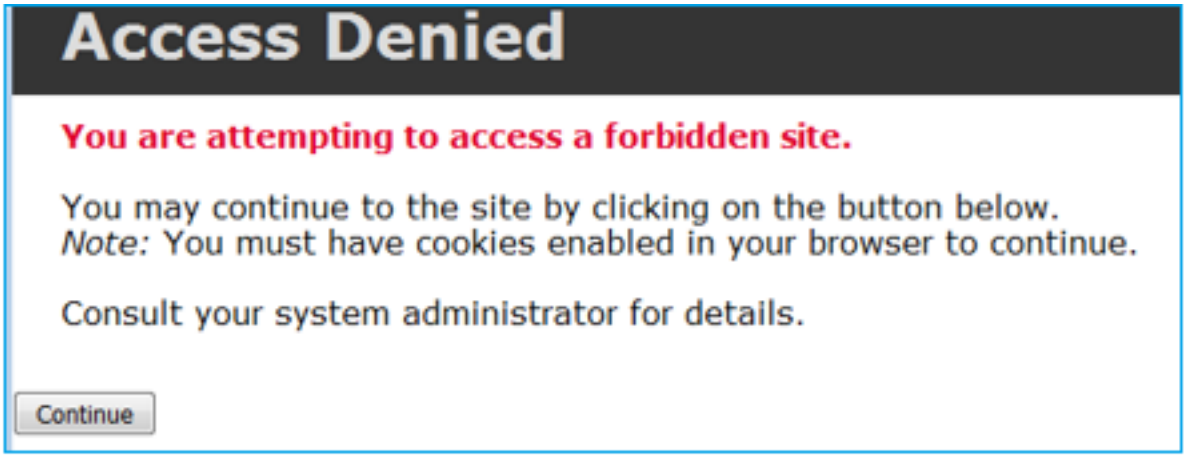
Le bloc interactif avec règle de réinitialisation est déployé sur le moteur FTD LINA en tant que **permit** et au moteur Snort comme règle d'initialisation :

```
firepower# show access-list
…
access-list CSM_FW_ACL_ line 9 remark rule-id 268438864: L7 RULE: Inter-Block-Rule1
access-list CSM_FW_ACL_ line 10 advanced permit tcp 192.168.10.0 255.255.255.0 host
192.168.11.50 eq www rule-id 268438864 (hitcnt=13) 0xba785fc0
access-list CSM_FW_ACL_ line 11 remark rule-id 268438865: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268438865: L7 RULE: Inter-Block_Rule2
access-list CSM_FW_ACL_ line 13 advanced permit ip 192.168.10.0 255.255.255.0 host 192.168.11.51
rule-id 268438865 (hitcnt=0) 0x622350d0
```

Moteur du renifleur :

```
# Start of AC rule.
268438864 intreset any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6
# End rule 268438864
268438865 intreset any 192.168.10.0 24 any any 192.168.11.51 32 any any any (appid 676:1)
(ip_protos 6, 17)
# End rule 268438865
```

Tout comme l'option Bloquer avec réinitialisation, l'utilisateur peut sélectionner **Continue** option :



Dans le débogage du renifleur, l'action est indiquée dans la réinitialisation interactive :

```
> system support trace

Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.52
Please specify a client port:
Please specify a server IP address: 192.168.11.50
Please specify a server port:
Monitoring packet tracer and firewall debug messages


192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 3232128039
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 new firewall session
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0 -> 0, vlan 0, source sgt type: 0, source
sgt tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest sgt tag: 0, svc 0, payload 0, client 0,
misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 match rule order 2, 'Inter-Block-Rule1',
action Interactive Reset
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 MidRecovery data sent for rule id:
268438864,rule_action:8, rev id:1099034206, rule_match flag:0x0
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 HitCount data sent for rule id: 268438864,
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
PASS

192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 Packet: TCP, SYN, ACK, seq 2228213518, ack
3232128040
192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
```

```
192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
PASS

192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 3232128040, ack
2228213519
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
PASS

192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 3232128040, ack
2228213519
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt
tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589,
misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 match rule order 2, 'Inter-Block-Rule1',
action Interactive Reset
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 bypass action sending HTTP interactive
response of 1093 bytes
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive block rule, 'Inter-
Block-Rule1', drop
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions
queue, drop
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 deleting firewall session flags = 0x800,
fwFlags = 0x1002
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
BLACKLIST
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 ===> Blocked by Firewall
Verdict reason is sent to DAQ
```

Àce stade, la page de blocage est affichée à l'utilisateur final. Si l'utilisateur sélectionne **Continue** (ou actualise la page web) la même règle que celle qui autorise cette fois le trafic :

```
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 1593478294, ack
3135589307
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt
tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589,
misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 match rule order 2, 'Inter-Block-Rule1',
action Interactive Reset
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 bypass action interactive bypass
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 allow action
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: allow rule, 'Inter-Block-Rule1',
allow
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive bypass rule, 'Inter-
Block-Rule1', allow
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 14, NAP id 1, IPS id 0, Verdict
PASS

192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 3135589307, ack
1593478786
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Firewall: allow rule, 'Inter-Block-Rule1',
allow
```

```
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Firewall: interactive bypass rule, 'Inter-
Block-Rule1', allow
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Snort id 14, NAP id 1, IPS id 0, Verdict
PASS
```

Interactive Block (blocage interactif) avec règle de réinitialisation envoie un message de réinitialisation du protocole TCP au trafic non Web :

```
firepower# show cap CAPI | i 11.50
   2: 22:13:33.112954       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: S
3109534920:3109534920(0) win 29200 <mss 1460,sackOK,timestamp 3745225378 0,nop,wscale 7>
   3: 22:13:33.113626       802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: S
3422362500:3422362500(0) ack 3109534921 win 8192 <mss 1380,nop,wscale 8,sackOK,timestamp
53252448 3745225378>
   4: 22:13:33.113824       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362501 win 229 <nop,nop,timestamp 3745225379 53252448>
   5: 22:13:33.114953       802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P
3422362501:3422362543(42) ack 3109534921 win 256 <nop,nop,timestamp 53252448 3745225379>
   6: 22:13:33.114984       802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P
3422362543:3422362549(6) ack 3109534921 win 256 <nop,nop,timestamp 53252448 3745225379>
   7: 22:13:33.114984       802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P
3422362549:3422362570(21) ack 3109534921 win 256 <nop,nop,timestamp 53252448 3745225379>
   8: 22:13:33.115182       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362543 win 229 <nop,nop,timestamp 3745225381 53252448>
   9: 22:13:33.115411       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362549 win 229 <nop,nop,timestamp 3745225381 53252448>
  10: 22:13:33.115426       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362570 win 229 <nop,nop,timestamp 3745225381 53252448>
  12: 22:13:34.803699       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: P
3109534921:3109534931(10) ack 3422362570 win 229 <nop,nop,timestamp 3745227069 53252448>
  13: 22:13:34.804523       802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: R
3422362570:3422362570(0) ack 3109534931 win 0
```

Connexions secondaires FTD et Trous D'Épingle

Dans les versions antérieures (par exemple 6.2.2, 6.2.3, etc.), le moteur Snort n'ouvre pas de trous d'épingle pour les connexions secondaires (par exemple FTD Data) si vous utilisez le **Trust** action. Dans les versions récentes, ce comportement est modifié et le moteur Snort ouvre des trous d'épingle même avec le **Trust** action.

Règles de Cisco Firepower Threat Defense (FTD)

- Utilisez les règles Prefilter Policy Fastpath (Fastpath pour la politique de préfiltre) pour les flux volumineux et pour réduire la latence à travers la boîte
- Utilisez les règles Prefilter Block (blocage du préfiltre) pour le trafic qui doit être bloqué en fonction des conditions L3/L4
- Utilisez les règles Trust (confiance) de la politique de contrôle d’accès si vous souhaitez contourner de nombreuses vérifications du renifleur, tout en profitant de fonctionnalités telles que la politique d’identité, la qualité du service, la fonction Security Intelligence, la détection d’applications et le filtre d’URL
- Placez les règles qui affectent moins les performances du pare-feu au sommet de la politique de contrôle d’accès avec l’utilisation de ces directives :

1. Règles Block (blocage) (couches 1 à 4) – Blocage de préfiltre

2. Règles Allow (autorisation) (couches 1 à 4) – Fastpath pour le préfiltre
3. Règles Block (blocage) de la politique de contrôle d'accès (couches 1 à 4)
4. Règles Trust (confiance) (couches 1 à 4)
5. Règles Block (blocage) (couches 5 à 7 – détection des applications, filtrage des URL)
6. Règles Allow (autorisation) (couches 1 à 7 – détection d'applications, filtrage d'URL, politique d'intrusion/politique de fichiers)
7. Règle Block (blocage) (règle par défaut)

- Évitez les connexions excessives (connectez-vous au début ou à la fin et évitez les deux en même temps)
- Soyez conscient de l'extension des règles, pour vérifier le nombre de règles dans LINA

```
firepower# show access-list | include elements
access-list CSM_FW_ACL_; 7 elements; name hash: 0x4a69e3f3
```

Résumé

Actions du préfiltre

Rule Action (FMC UI)	LINA Action	Snort Action	Notes
Fastpath	Trust	Fastpath	Static Flow Offload to SmartNIC (4100/9300). **No packets** are sent to Snort engine.
Analyze	Permit	-	The ACP rules are checked. **Few** or **all packets** are sent to Snort engine for inspection. Traffic is allowed or dropped based on Snort engine verdict
Block (Prefilter)	Deny	-	Early drop by FTD LINA **No packets** are sent to Snort engine

Actions de la politique de contrôle d'accès

Rule Action (FMC UI)	Additional Conditions	LINA Action	Snort Action	Notes
Block	The rule matches L3/L4 conditions	Deny	Deny	
Block	The rule has L7 conditions	Permit	Deny	
Allow		Permit	Allow	6.3+ supports Dynamic Flow Offload (4100/9300)
Trust	(SI, QoS, or ID) enabled	Permit	Fastpath	6.3+ supports Dynamic Flow Offload (4100/9300)
Trust	(SI, QoS, and ID) disabled	Trust	Fastpath	Static Flow Offload (4100/9300)
Monitor		Permit	Audit	Monitor Rule doesn't drop or permit traffic, but it generates a Connection Event. The packet is checked against subsequent rules and it is either allowed or dropped
Block with reset		Permit	Reset	When a packet matches Block with reset rule FTD sends a TCP Reset packet or an ICMP Type 3 Code 13 Destination Unreachable (Administratively filtered) message
Interactive Block		Permit	Bypass	Interactive Block Rule prompts the user that the destination is forbidden If bypassed, by default, the firewall allows to bypass the block for 600 seconds
Interactive Block with reset		Permit	Intreset	Same as Interactive Block with the addition of a TCP RST in case of non-web traffic

Note: À partir de la version 6.3 du code logiciel FTD, le déchargement de flux dynamique peut décharger les connexions qui répondent à des critères supplémentaires, par exemple, les paquets sécurisés qui nécessitent une inspection Snort. Consultez la section sur le déchargement des connexions volumineuses (flux) du Guide de configuration du centre de gestion Firepower Management Center pour plus de détails.

Informations connexes

- Règles de contrôle d'accès de Cisco FTD
- Préfiltres et politiques de préfiltre de Cisco FTD
- Analysez les captures de pare-feu Firepower pour résoudre efficacement les problèmes de réseau
- Utilisation des captures Cisco Firepower Threat Defense (FTD) et du traceur de paquet
- Configurez la connexion sur Cisco FTD à l'aide de Cisco FMC
- Support et documentation techniques - Cisco Systems
- Déchargement de connexions importantes

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.